2.7.5-1 User Confirmation of Destructive Entries

When a control entry will cause any extensive change in stored information, procedures, and/or system operation, and particularly if that change cannot be easily reversed, the user should be notified and confirmation of the action should be required before implementing it.
Additional Information: What constitutes "potentially destructive" requires definition in the context of each system operation. When user entries or changes will be nullified by an abort action, the user should be requested to confirm the abort. Confirmation messages should be simple, positive, and direct.[5908]

2.7.5-2 Informing Users of Potential Information Loss

For conditions that may require special user attention to protect against information loss, an explicit alert and/or advisory message should be provided to prompt appropriate user action.
Additional Information: The prompt for a CONFIRM action should inform users explicitly of any possible data loss. For example, the message, "CONFIRM deletion of entire FEEDWATER file?" is preferable to "CONFIRM DELETE." If a complete file is to be deleted, sufficient information (e.g., name, description, size, date established, and data last changed), should be displayed to verify the file for deletion.[5908]

2.7.5-3 Preventing Data Loss at Logoff

When a user requests logoff, pending transactions should be checked and if any pending transaction will not be completed, or if data will be lost, an advisory message requesting user confirmation should be displayed.
Additional Information: A user may sometimes suppose that a job is done before taking necessary implementing actions.[5908]

2.7.5-4 Displaying Data to be Changed

If a user requests change (or deletion) of a stored data item that is not currently being displayed, both the old and new values should be displayed so that the user can confirm or nullify the change before the transaction is completed.
Additional Information: For proposed deletion of significant amounts of data, such as entire files, it probably will not be feasible to display all of the data. In such instances, sufficient information should be provided so that users can identify those files they have selected for deletion. The user should be clearly advised of the potential data loss and required to confirm the destructive action before it will be executed. This practice will tend to prevent inadvertent change, including changes resulting in loss of needed data. User attempts at selective data change without displayed feedback will be prone to error.[5908]

2.7.6-1 Protection from Computer Failure

Automatic measures should be provided to minimize data loss from computer failure.
Additional Information: An automatic capability is needed because users cannot be relied upon to remember to take necessary protective measures. Though not strictly a feature of user interface design, reliable data handling by the computer will do much to maintain user confidence in the system. Conversely, data loss resulting from computer failure will weaken user confidence, and reduce user acceptance where system use is optional. For example, depending upon the criticality of the application, different protective measures may be justified, including periodic automatic archiving of data files, maintenance of transaction logs for reconstruction of recent data changes, offsite storage of copies of operating software, or even provision of parallel "backup" computing facilities.[5908]

2.7.6-2 Protection from Interrupts

When a proposed user action will interrupt a current transaction sequence, automatic means to prevent data loss should be provided.
Additional Information: If potential data loss cannot be prevented, the user should be informed. Interrupts should not be permitted without user confirmation. Some interrupt actions such as BACKUP, CANCEL, or REVIEW, by their definition will cause only limited data change, and so need no special protection. However, if an interrupt action may cause extensive data change (e.g., RESTART, LOGOFF), then the user should be required to confirm that action before processing. If a user should interrupt a series of changes to a data file, then the computer might automatically save both the original and the changed versions of that file for subsequent user review and disposition.[5908]

2.7.6-3 Protection from Data Change

When information must not be changed, users should not be permitted to change controlled items.
Additional Information: It is not enough simply to instruct users not to make changes in displayed information. Setpoints specified in plant technical specifications are an example of information that must not be changed.[5908]

2.7.6-4 Explicit Action to Select Destructive Modes

Users should take explicit action to select any mode of interaction that might result in data loss.
Additional Information: Destructive modes should not be established automatically. In many applications, it may be better not to provide any destructive mode. Instead of providing a DELETE mode, for example, require that DELETE be a discrete action subject to confirmation by the user when the requested data deletion is extensive.[5908]

2.7.6-5 Safe Defaults

If automatic defaults are provided for control entries, those defaults should protect against data loss, or at least not contribute to the risk of data loss.
Additional Information: For example, when printout of filed data is requested, one control option might be to delete that file after printing. The default value for such a destructive option should automatically be set to NO whenever the printing options are presented to a user for selection.[5908]

2.7.6-6 Protecting Physical Controls

If activation of function keys (and other control devices) may result in data loss, they should be located separately and/or physically protected to reduce the likelihood of accidental activation.[5908]

2.7.6-7 Disabling Unneeded Controls

When function keys and other devices are not needed for current control entry, and especially when they may have destructive effects, they should be temporarily disabled by the software so that they cannot be activated by a user.

Additional Information: Some means should also be provided to help users distinguish currently active from disabled controls, such as brightening (active) or dimming (disabled) their associated labels. If labeling is adequate, then user selection of a disabled control need produce no response. If adequate labeling cannot be provided, then user selection of a disabled control should produce an advisory message that the control is not currently active.[5908]

2.7.6-8 Distinctive File Names

When data files may be deleted (or overwritten) by name, the file names assigned by the system should be distinctive.[5908]

2.7.6-9 Feedback for Mode Selection

When the result of user actions will be contingent upon prior selection among differently defined modes of interaction, a continuous indication of the current mode should be provided, particularly when user inputs in that mode might result in data loss.

Additional Information: A user cannot be relied upon to remember prior actions. Thus, any action whose results are contingent upon previous actions can represent a potential threat to data protection. For example, if a DELETE mode is being used to edit displayed data, some indication of that mode should be continuously displayed to the user.[5908]

2.7.6-10 Protection from Interference by Other Users

Data should be protected from inadvertent loss caused by the actions of other users.

Additional Information: When one user's actions can be interrupted by another user, that interruption should be temporary and nondestructive. The interrupted user should subsequently be able to resume operation at the point of interruption without data loss. When multiple users review, enter, or modify data in a system, they should be able to review and browse data changes or entries made by other users. In systems where information handling requires the coordinated action of multiple users, it may be appropriate that one user can change data that will be used by others. However, when multiple users will act independently, then care should be taken to ensure that they will not interfere with one another.[5908]

2.7.6-11 Segregating Real from Simulated Data

When simulated data and system functions are displayed or provided (perhaps for user training), real data should be protected and real system use should be clearly distinguished from simulated operations.[5908]

2.7.6-12 Data Entry/Change Transaction Records

In situations where unauthorized data changes may be possible, users (or a system administrator) should be able to request a record of data entry/change transactions.

Additional Information: Transaction records might be maintained for purposes of user guidance as well as for data protection.[5908]

2.7.7-1 Acknowledging Corrections

All error corrections by the user should be acknowledged by the system, either by indicating a correct entry has been made or by another error message.[5908]

2.7.7-2 UNDO to Reverse Control Actions

Any user action should be immediately reversible by an UNDO command.
Additional Information: UNDO itself should be reversible, so that a second UNDO action will do again whatever was just undone. Even with an UNDO capability, however, a user may make an irretrievable mistake, if succeeding actions intervene before a prior destructive action is noticed. If a user is too hasty in confirming a destructive action, and realizes the mistake right away (i.e., before taking another action), then an UNDO action might be taken to reverse the damage.[5908]

2.7.7-3 User Review and Editing of Entries

For all inputs, whether data entries or commands, users should be allowed to edit composed material before requesting computer processing.
Additional Information: Input editing will allow users to correct many errors before computer processing. When an error is detected, a user will be able to fix it by editing, i.e., without having to retype any correct items (which might introduce further errors).[5908]

2.7.7-4 Immediate Error Correction

When the system detects an error in a user input, the user should be allowed to make an immediate correction.
Additional Information: It is helpful to correct data entry errors at the source, i.e., while a user still has the entry in mind and/or source documents at hand. When a user cannot correct an entry, as when transcribing from a source document that itself contains an error, it may help to allow the user to defer entry of the wrong item. Alternatively, the user might wish to cancel the transaction.[5908]

2.7.7-5 Editing Entries After Error Detection

Following error detection, users should be allowed to edit entries by rekeying only those portions that were in error.
Additional Information: If a user must re-enter an entire data set to correct one wrong item, new errors may be made in previously correct items.[5908]

2.7.7-6 Explicit Entry of Corrections

Users should be required to take an explicit ENTER action for computer processing of error corrections.
Additional Information: The action taken to accomplish corrections should be the same action that was taken to enter the data originally.[5908]

2.7.7-7 Automated Correction Aid

When inappropriate or unrecognized commands are detected, a list should be provided to the user showing permissible commands, anticipating the command intended.[5908]

2.7.7-8 Flexible BACKUP for Error Correction

Users should be allowed to BACKUP easily to previous steps in a transaction sequence in order to correct an error or make any other desired change.

Additional Information: For example, a user might wish to BACKUP through the defined sequence of a question-and-answer dialogue in order to change a previous answer.[5908]

2.7.7-9 Errors in Stacked Commands
If an error is detected in a stacked series of command entries, the computer should either consistently execute to the point of error, or else consistently require users to correct errors before executing any command.
Additional Information: In most applications, partial execution will probably prove desirable. The point here is that an interface design decision should be made and then followed consistently.[5908]

2.7.7-10 Partial Execution of Stacked Commands
If only a portion of a stacked command can be executed, the user should be notified and provided appropriate guidance to permit correction, completion, or cancellation of the stacked command.
Additional Information: Note that stacked commands can fail because of error in their composition, or for other reasons such as unavailability of required data.[5908]

2.7.7-11 Replacing Erroneous Commands
If a user makes a command entry error, after the error message has been displayed, the user should be allowed to enter a new command.
Additional Information: A user should not be forced to correct and complete an erroneous command. In considering a command entry error message, a user may decide that the wrong command was chosen in the first place, and wish to substitute another command instead.[5908]

2.7.7-12 Correcting Command Entry Errors
If a command entry is not recognized, the user should be allowed to revise the command rather than rejecting the command outright.
Additional Information: Misstated commands should not simply be rejected. Instead, software logic should guide users toward proper command formulation.[5908]

2.7.8-1 On-Line Guidance
Reference material describing system capabilities, procedures, and commands and abbreviations, should be available on-line.
Additional Information: Design of user guidance should be consistent with system security restrictions.[5908]

2.7.8-2 Access to Guidance
Explicit actions should be required to access or suppress user guidance.[5908]

2.7.8-3 HELP Request
At any point in an interaction, users should be able to access on-line user guidance by means of a simple action that is consistent throughout the interface.
Additional Information: Users should have multiple methods of requesting help. For example, a user might (1) select Help in a pull-down menu, (2) type a "Help" command, and/or (3) press a Help Function Key.[5908]

2.7.8-4 HELP Guidance
Advisory messages or prompts should be available to guide users in accessing help messages.
Additional Information: An on-line HELP index should be provided.[5908]

2.7.8-5 Synonyms for Standard Terminology
When a user requests HELP on a topic, the computer should accept synonyms and abbreviations.[5908]

2.7.8-6 Context-Sensitive HELP
The information presented in response to a HELP request should be tailored to the task context.
Additional Information: If an error in command entry is made, HELP should display information concerning that command, its function, its proper structure and wording, and required and optional parameters.[5908]

2.7.8-7 Clarifying HELP Requests
When a request for HELP is ambiguous in context, the computer should initiate a dialogue to specify what data, message, or command requires explanation.
Additional Information: In order to define the needed information, the user might be allowed to point at a displayed item about which HELP then would be provided.[5908]

2.7.8-8 Multilevel HELP
When a HELP display provides summary information, more detailed explanations should be available.[5908]

2.7.8-9 Browsing HELP
Users should be able to browse on-line HELP.[5908]

2.7.8-10 Return from HELP
The user should be able to easily return to the task after accessing HELP.[5908]

2.7.8-11 Hardcopy Procedures
A complete hardcopy set of computer system operating procedures and contingency procedures should be available in the control room.

Additional Information: Operating procedures should describe the overall computer system, the components with which the user can interface, and the specific procedures necessary to accomplish all of the user-computer interface functions. Contingency procedures should describe indications available to the user which identify failure or malfunctioning of the computer system and necessary actions to be performed by the user if the computer fails or malfunctions.[0700]

2.7.8-12 Computer System Procedures
Procedures should be prepared from the point of view of the user.[0700]

2.7.8-13 Display Indices
Cross-indices of the available data displays should be available in the control room in hardcopy form.
Additional Information: The specific codes, or addresses, by which data displays can be called up by a user should be cross-indexed by alphanumeric or numeric code, program name, system/subsystem identification, and functional group identification.[0700]

2.8-1 Appropriate Use of HSI Flexibility Features

Flexible HSI features should be provided when they provide specific benefits to user tasks and their use does not impair user performance.

Additional Information: User performance may be impaired by an excessive number of flexibility features or inadequately designed flexibility features that create demands that compete with primary tasks. Inadequately designed flexibility features can also expose the user to HSI configurations that violate human factors engineering principles and may increase the likelihood of errors and poorer task performance. Table 2.6 lists some uses of HSI flexibility that may enhance performance.[6546]

Table 2.6 Uses of HSI flexibility

Reduce the Cost of Accessing Information – Flexible HSI capabilities can reduce the attention and effort required for accessing information. The flexibility of computer-based technologies can enhance operator performance by allowing the HSI to provide the right information for the operator's current work methods and work objectives, while removing unneeded information that may become a nuisance. Examples include: automated information retrieval features; programmable function keys for accessing particular displays; capabilities for organizing information (i.e., display window management, spatial arrangement of icons); and capabilities for introducing labels, markers, or landmarks to support operators in locating information in displays that require visual scanning.

Reduce the Cost of Processing and Integrating Information – Flexible HSI capabilities can support operators in mentally processing and integrating information presented by the HSI. Examples of HSI features for arranging the spatial proximity of information to aid mental integration include: the physical movement of display devices, the movement of display pages to particular display devices, and the movement of display pages within display windows. Examples of HSI features for supporting users interpreting information include reconfigurable displays, such as graphical plots in which an operator may plot one variable as a function of another or as a function of time, and features that perform calculations requested by the operator.

Reduce the Cost of Executing Control Actions – Flexible HSI capabilities can reduce the effort and attention required for executing control actions. Examples include HSI features that allow particular control actions to be executed automatically. Other examples include: "escape mechanisms" features, which allow to the operator to promptly terminate and exist complicated human-system interactions, and "workarounds," which allow the user to override automatic responses that may not be beneficial for a particular task.

Enhance Signals – This capability increases the salience of an indication or piece of information to support detection by operators. These changes in salience effectively increase the signal-to-noise ratio for specific information.

Reduce Noise – This capability reduces or removes "noise" from the information environment to support the operator in detecting relevant information. This removal or reduction of noise effectively increases the signal-to-noise ratio for other information that may be more important. Noise may include indications of plant or system changes that do not provide information that is useful to the operator's current tasks.

Document a Baseline or Trend – This capability allows the operator to create a referent for monitoring so that changes can be easily identified without relying upon the operator's memory of the previous state. Examples include capabilities for documenting initial conditions or for establishing a trend over a period of time for comparison at some later time.

Create External Reminders – This capability allows the operator to create reminders for activities involved in monitoring or control execution. Reminders for monitoring activities may identify particular variables requiring close attention. Reminders for control actions may remind operators of special conditions important when carrying-out control actions. For example, operators may create reminders regarding unusual control configurations that should not be changed or to draw attention to unusual indications that are already being addressed in other ways. These reminders may be created through manipulations of the appearance of the HSI component or through the creation of messages.

2.8-2 Design for User Requirements

Users should not have to use flexible interface features to support tasks and circumstances that could have been anticipated and designed for.

Additional Information: The flexible user interface features provided should be the result of careful analyses of user requirements. A flexible user interface feature should address the need to optimize performance under specific conditions. They should not be a substitute for analyses of user requirements. Flexibility without proper analysis can expose the user to configurations that may impair performance, such as by increasing the likelihood of errors or delays.[6546]

2.8-3 Scope of Flexibility

The system should be sufficiently flexible to enable users to respond to unanticipated situations or where personal preference can positively impact performance.

Additional Information: Users should be able to develop novel information displays for unusual circumstances.[6546]

2.8-4 Limits to Flexibility

Users' flexibility in configuring the interface should not be unlimited.

Additional Information: Flexibility should be constrained so that working with the system does not become a complex decision-making task. The options provided to be user for configuring the interface should be well defined.[6546]

2.8-5 Default Configuration and HSI Flexibility Features

Displays that can be modified by users should provide a means for the user to rapidly return the display to its default configuration.[6546]

2.8-6 Changes to Display Characteristics

Users should not be able to change display characteristics that have been specifically designed to convey information important to their tasks.

Additional Information: The HSI may allow users to change or adjust some characteristics of the HSI, if these changes will enhance personnel performance. However, users should not be able to change display characteristics that have been specifically designed to convey important information, such as coding schemes. Examples for graphical elements include size, shape, and color codes for icons, symbols, borders, lines, and arrows. Examples for text elements include font characteristics (e.g., size, style, and color), abbreviations and acronyms for messages and labels.[6546]

2.8-7 User Expertise and HSI Flexibility Features

The design of flexible HSI features should provide capabilities that are consistent with the levels of expertise of the users.

Additional Information: User needs are typically different for different levels of expertise. Users who have limited exposure to the advanced capabilities of computer-based HSI components may require a high degree of support for interface management actions, such as through the use of menu-based systems and computer-based help features. Users who are highly proficient in the use of the HSI may require features that limit the number of steps required to complete an action, such as via a command-based interface rather than a menu-based interface.[6546]

2.9.1-1 Automated Security Measures

When required, automated measures to protect data security should be provided, relying on computer capabilities rather than on more fallible human procedures.

Additional Information: For protection against unauthorized users, who may be intruders in a system, the need for automated security measures is clear. For legitimate users, the need for data protection is to minimize data loss resulting from potentially destructive equipment failures and user errors. Even careful, conscientious users will sometimes make mistakes, and user interface logic should be designed to help mitigate the consequences of those mistakes.[5908]

2.9.1-2 Notification of Threats to Security

Messages or signals should be provided in order to notify users (and system administrators) of potential threats to data security (i.e., of attempted intrusion by unauthorized users).

Additional Information: For protecting data from unauthorized use, it may not be enough merely to resist intrusion. It may also be helpful if the computer can detect and report any intrusion attempts. In the face of persistent intrusion attempts, it may be desirable to institute countermeasures of some sort, such as changing user passwords or establishing other more stringent user authentication procedures.[5908]

2.9.1-3 Auxiliary Tests to Authenticate User Identity

When system security requires more stringent user identification than is provided by password entry, auxiliary tests should be devised that authenticate user identity without imposing impractical demands on the user's memory.[5908]

2.9.1-4 Easy Logon

The logon process and procedures for user identification should be as simple as possible, consistent with protecting the system and associated data.

Additional Information: The logon process should provide prompts for all user entries, including passwords and/or whatever other data are required to confirm user identity and to authorize access to the system. Authentication of user identity is generally not enhanced by requiring a user to enter routine data such as terminal, telephone, office, or project numbers. In most organizations, those data can readily be obtained by other people. If verification of those data is needed, the user should be asked to review and confirm currently stored values in a supplementary procedure following logon.[5908]

2.9.1-5 Private Entry of Passwords

When a password must be entered by a user, password entry should not be displayed.

Additional Information: Covert entry of passwords will prevent casual eavesdropping by onlookers. This represents an exception to the general recommendation that all entries should be displayed. Special characters (e.g., * or #) may be displayed with each keystroke rather than the actual characters being entered. Alternatively, blanks may be displayed accompanied by an audio cue (e.g., a click or beep) for keystroke feedback.[5908]

2.9.1-6 User Choice of Passwords

When passwords are required, users should be allowed to choose their own passwords and to change their passwords as needed.

Additional Information: Where data protection is critical, user selected passwords should be tested against a list of common passwords (for example, "me," car types, names spelled backwards "nhoj," or birth dates). A password chosen by a user will generally be easier for that individual to remember. Security is enhanced if users are readily able to change their passwords, e.g., a user may suspect that a password has been disclosed, and thus may wish to change it.[5908]

2.9.1-7 Limiting Unsuccessful Logon Attempts
A maximum limit on the number and rate of unsuccessful logon attempts should be imposed.
Additional Information: These limits should provide a margin for user error while protecting the system from persistent attempts at illegitimate access. A record of continuing failure by any particular user to complete successful logon procedures, including password entry and other tests of claimed user identity, may indicate persistent intrusion attempts or lack of fitness for duty. Thus, repeated logon failures might be grounds for denying access to that user. Access might be denied temporarily for some computer-imposed time interval, or indefinitely, pending review by a system administrator. Legitimate users will sometimes have difficulty completing a successful logon, perhaps due to inattention, or a faulty terminal, or faulty communications. Occasional logon failures of that kind should be tolerable to the system, with the user simply invited to try again.[5908]

2.9.1-8 Continuous Recognition of User Identity
Once a user's identity has been authenticated, any authorized data access/change privileges are for that user should continue throughout a work session.
Additional Information: If an identified user is required to take separate actions to authenticate data handling transactions, such as accessing particularly sensitive files or issuing particular commands, the efficiency of system operations may be degraded. Where continuous verification of user identity seems required for data protection, some automatic means of identification might be employed for that purpose.[5908]

2.9.1-9 Single Authorization for Data Entry/Change
User authorization should be established at initial logon.[5908]

2.9.1-10 Logging On
When users must log on to a system, logon should be a separate procedure that is completed before a user may select any operational options.[5908]

2.9.1-11 Logon Frame
The logon frame should appear as soon as possible on the display with no additional user involvement.[5908]

2.9.1-12 Logon Delays
Logon delays should be accompanied by an advisory message to tell the user its current status and when the system will become available.[5908]

2.9.1-13 Immediate Start of Productive Work
After completing the logon process, the user should be able to start productive work immediately.[5908]

2.9.1-14 Logging Off
If there are pending actions and the user requests a logoff, the system should inform the user that these actions will be lost and allow the user to cancel either the pending actions or the logoff.[5908]

2.9.1-15 Saving Open Files in Automatic Logoff

Where possible, in the event of automatic logoff, open files should be saved to some defined file name. *Additional Information:* For example, by concatenation of User's Name + Date.[5908]

2.9.1-16 Automatic Logoff

Interactive timesharing systems should allow some specified time between keyboard actions before automatic logoff unless a longer period is requested by the user.[5908]

2.9.1-17 Audible Signal for Automatic Logoff

An audible signal should be presented at specified intervals prior to automatic logoff.[5908]

2.9.2-1 Encryption

When sensitive data may be exposed to unauthorized access, a capability for encrypting those data should be provided.

Additional Information: Since potential exposure may be assumed during any external data transmission, encryption should be imposed routinely by the computer. Users should not be relied upon to request encryption. For protection of data within a shared system, a user might choose to encrypt private files to prevent their reading by other people. In such a case, the user must specify a private encryption "key," which will then serve as the basis for automatic encryption by the computer.[5908]

2.9.2-2 Ensuring Reversible Encryption

Encrypted data should be protected from any change that might prevent successful reversal of their encryption.[5908]

2.9.2-3 Displayed Security Classification

When displayed data are classified for security purposes, a prominent indication of security classification should be included in each display.

Additional Information: Where a display includes partitioned "windows" of data from different sources, it may be necessary to label security classification separately for each window. Under those conditions, some form of auxiliary coding (e.g., color coding) might help users distinguish a window that contains data at a high security level. This practice will serve to remind users of the need to protect classified data, both in access to the display itself and in any further dissemination of displayed data.[5908]

2.9.2-4 Display Suppression for Security

When confidential information is displayed at a workstation that might be viewed by casual onlookers, the user should be provided with some rapid means of temporarily suppressing a current display if its privacy is threatened, and then resuming work later.

Additional Information: A suppressed display should not be entirely blank, but should contain an appropriate message indicating its current status, e.g., "Display is temporarily suppressed; enter password to resume work." Such a capability is sometimes called a "security pause." For quick display suppression, a function key might be provided. To retrieve a suppressed display and resume work, a user might be required to make a code entry such as a password, in the interests of data protection.[5908]

2.9.2-5 Protecting Printed Data

As required for security, procedures to control access to printed data should be established, rather than simply prohibiting the printing of sensitive data.

Additional Information: User requirements for printed data are often unpredictable, and printing restrictions may handicap task performance. Rather than restrict printing, establish appropriate procedures for restricting further distribution of data printouts.[5908]

2.9.2-6 Protecting Display Formats

Display formatting features, such as field labels and delimiters, should be protected from accidental change by users.

Additional Information: In many data entry tasks, users will be allowed to change data fields but should be prevented from making any structural changes to the display. In applications where a user may have to create or modify display formats, special control actions should be provided for that purpose.[5908]

2.9.2-7 Protecting Displayed Data

When protection of displayed data is essential, computer control over the display should be maintained.
Additional Information: It is not enough simply to instruct users not to make changes in displayed data. Users may attempt unwanted changes by mistake, or for curiosity, or perhaps even to subvert the system.[5908]

2.9.2-8 Indicating 'Read-Only' Displays

When users are not authorized to change displayed data, "read-only" status should be indicated on the display.
Additional Information: In applications where the use of read-only displays is common, some simple cue in the display header may suffice to indicate that status. In applications where users can usually make additions and/or corrections to displayed data, any exception to that practice may confuse a user and so should be noted more prominently on the display.[5908]

2.9.2-9 Automatic Records of Data Access

When records of data access are necessary, the records should be maintained automatically.
Additional Information: Transaction records and logs should be stamped with user identifiers, time, and date. Provisions should be made to control requests for records and logs of data transactions with classified material. Users should be informed concerning the nature and purpose of automated recording of individual actions. Even cooperative, well-intentioned users can forget to keep manual logs of data access, and will resent the time and effort required to keep such logs. Subversive users, of course, cannot be expected to provide accurate records.[5908]

SECTION 3: CONTROLS

3 CONTROLS

Controls are the devices through which personnel interact with the HSI and the plant, including computer-input devices and conventional controls. Each is described below. General design and coding principles that apply to all controls are given in Section 3.1. Soft controls are treated as an HSI system (see Section 7) because they have display, interactions, and control components.

COMPUTER-BASED INPUT DEVICES

Input devices are devices used to provide input to computer-based systems. The following input devices are frequently used in computer-based systems:

Alphanumeric keyboards

These are keypads containing alphabetic and numeric characters. The user presses these keys to form commands or to enter data. Review guidelines for alphanumeric keyboards are presented in Section 3.2.1.

Function keys

This refers to the physical keys of a keyboard or keypad that are used to initiate a particular, dedicated function. Review guidelines for function keys are presented in Section 3.2.2. (The user-system interaction characteristics of function keys are addressed in Section 2.)

Trackballs, Joysticks, and Mice

These are indirect pointing devices in the sense that their movement at one location causes the cursor to move at a separate location – the display screen. A trackball is a device that allows the user to control the cursor's movement in any direction by rotating a ball. A joystick is a stick-type device that can provide continuous control of the cursor in any direction on a display screen. A mouse is a device whose movements across a flat surface are converted into analogous movements of the cursor across the screen. Review guidelines for trackballs, joysticks, and mice are presented in Section 3.2.3.

Touchscreens, Light Pens, and Graphics Tablets

These are direct pointing devices in that they allow the user to select information directly from a display screen. A touch screen is a device whereby user can communicate with the computer by touching a screen. A light pen is a pencil- or pen-like device that interacts with the computer system through the display device screen by either emitting or sensing light. A graphics tablet (also called a digitizing tablet) is a device that converts an image into digital code by drawing or tracing with a pen-like or puck-like instrument. The instrument is moved across the tablet, generating a series of X-Y coordinates. Review guidelines for touchscreens, light pens, and graphics tablets are provided in Section 3.2.4.

Speech input devices

These devices allow the user to provide input in spoken form, which a computer then interprets as data or commands. A speech input system typically consists of a microphone (e.g., stationary or mounted to a headset), components for transmission (e.g., a cable or a wireless media), and a processing unit. Review guidelines for speech input are provided in Section 3.2.5.

CONVENTIONAL CONTROL DEVICES

Conventional controls are hardwired devices for providing control input. Each control typically has a single dedicated location in a control panel. Conventional controls usually have either discrete settings or a continuous range for adjustment. Those with discrete settings typically have one of two types of operation – momentary and latching. Momentary control returns to its original setting when released. A

latching control stays in position until operated again. The following are examples of conventional control devices:

Pushbutton controls

These are buttons that generate a signal when they are pressed with the finger or hand. Their shape (e.g., round or square), size, and texture may vary. Legend pushbuttons are illuminated by internal lamps; their faces may contain alphanumeric text. Review guidelines for pushbutton controls are provided in Section 3.3.1.

Rotary controls

These controls are operated with a rotary motion. They include knobs, dials, J-handle controls, key-operated controls, continuous adjustment controls, and rotary selector controls. Review guidelines for rotary controls are provided in Section 3.3.2.

Other Controls

Thumbwheels

These controls are wheels that are turned by running the thumb or finger across their surface. Review guidelines for thumbwheels are provided in Section 3.3.3.1.

Slide switches

These controls are operated by sliding a knob linearly in the horizontal or vertical direction. Review guidelines for slide switches are provided in Section 3.3.3.2.

Toggle switches

These are stemmed switches that the user can move to discrete settings. Review guidelines for toggle switches are provided in Section 3.3.3.3.

Rocker switches

These switches have nearly flat faces and can be moved by the user to discrete settings. Review guidelines for rocker switches are provided in Section 3.3.3.4.

3.1.1-1 Appropriate Use of Input Devices

Input and control devices provided for interacting with the HSI should be appropriate for the user's task requirements.

Additional Information: Control/input devices and conditions for their appropriate use are listed in Table 3.1.[5908]

Table 3.1 Control and input devices for human-computer interaction

Control/Input Device	Conditions for Appropriate Use
Cursor Control Keys	Moving cursor in X and Y dimensions
Touch Screen	Moving/holding arm to screen for long periods of time is not required Screen does not have small poke points relative to size of finger tip A low level of resolution is required for positioning Task will not be disrupted by hand temporarily blocking screen Periodic cleaning of screen is provided
Light Pen	High positioning precision is not required Holding arm to screen for long periods of time is not required
Mouse	Adequate space is available for mouse movement over a pad or desktop A low to medium level of resolution is required for positioning Periodic cleaning is provided
Isotonic Joystick (Displacement)	Positioning accuracy is more important that positioning speed
Trackball	Rapid cursor positioning is desirable Limited space is available for installing an input device
Graphics Tablet	A low to medium level of resolution is required
Isometric Joystick (Force)	Precise or continuous control of two or more related dimensions is required

3.1.1-2 Input Device Stability

Input and control devices should be stable during normal usage, i.e., they should not slip or rock, unless such actions are a part of the controller operation.[5908]

3.1.1-3 Feedback

Visual or auditory feedback should be provided to indicate that the system has received a control input.

Additional Information: This is especially important when the control surface does not depress or move (such as with a force joystick or touchscreen), thereby providing little tactile feedback to the user.[5908]

3.1.1-4 Accidental Input or Actuation Prevention

The system should be located and designed to prevent the accidental manipulation of control and input devices that could result in changes to the status of the system functions, components, or data.
Additional Information: Controls may be recessed, shielded, or otherwise surrounded by physical barriers. The control should be entirely contained within the envelope described by the recess or barrier. Controls may be covered or guarded with movable (e.g., hinged) barriers. Safety or lock wires should not be used. When a movable control guard is in the open position, it should not interfere with the operation of the guarded control or other adjacent controls. Conventional controls may be provided with interlocks. The interlocking controls may require: (1) extra movement (e.g., a side movement out of a detent position or a pull-to-engage clutch), or (2) prior operation of a related or locking control.[5908, 0700]

3.1.1-5 Location

Controls should be operable from the location where the user is most likely to need to interact with the system.[0700]

3.1.1-6 Speed

Controls should provide rapid positioning of cursors or selection of choices.[0700]

3.1.1-7 Accuracy

The accuracy of the control device or method should be commensurate with the functions to be served.[0700]

3.1.1-8 Displacement

Control design should allow the user freedom of movement to perform other duties.[0700]

3.1.1-9 Range and Precision

Control should provide the sufficient range and precision required by the task.[0700]

3.1.1-10 Economy

Each control or input device should be necessary, use minimal space, and be the simplest effective control for the task concerned.
Additional Information: There should be a good reason to require a control for the function concerned. Duplication of controls should not occur, except for a specific reason. The precision and range of a control should not greatly exceed the need.[0700]

3.1.1-11 Human Suitability

Controls and input devices should be suitable for use in a control room environment.
Additional Information: Controls and input devices should be suited to the anthropometric and ergonometric characteristics of the expected user population. Each should be recognizable in terms of its function and should be of the type normally anticipated for the operation concerned. This means conforming to user expectations, matching to other devices having similar functions, and generally conforming to conventional practice.[0700]

3.1.1-12 Compatibility with Emergency Gear

If used while wearing protective equipment (e.g., oxygen masks and protective gloves), controls and input devices should be easy to identify and activate, or use.[0700]

3.1.1-13 Durability

Controls and input devices should be sufficiently rugged to withstand normal and emergency use.

Additional Information: Each device should retain its appearance, "feel," and functional characteristics during its service life. Broken, chipped, or crumbled control surfaces should not ordinarily occur. Control knobs or handles should not rotate, slip, or move loosely on their shafts. No internal wear or breakage should occur which alters the "feel" or other sensory feedback of a control. Controls should not develop internal looseness, binding, or backlash.[0700]

3.1.1-14 Control Activation
Controls and input devices should require distinct or sustained effort for activation.
Additional Information: Conventional controls should be provided with resistance (e.g., friction or spring-loading). Activation of computer-displayed controls should require a separate action, distinct from pointing.[0700]

3.1.1-15 Sequential Activation
When a strict sequential activation is necessary, controls should be provided with locks to prevent the controls from passing through a position.
Additional Information: Movement to the next position should require a new control action.[0700]

3.1.1-16 Population Stereotypes
Control movements should conform to population stereotypes (see Figure 3.1).
Additional Information: The following are control movement stereotypes for the U.S. population: (1) On, start, run, open; Up, right, forward, clockwise, pull; (2) Off, stop, close; Down, left, backward, counterclockwise, push; (3) Right; Clockwise, right; (4) Left; Counterclockwise, left; (5) Raise; Up; (6) Lower; Down; (7) Increase; Forward, up, right, clockwise; (8) Decrease; Backward, down, left, counterclockwise.[0700]

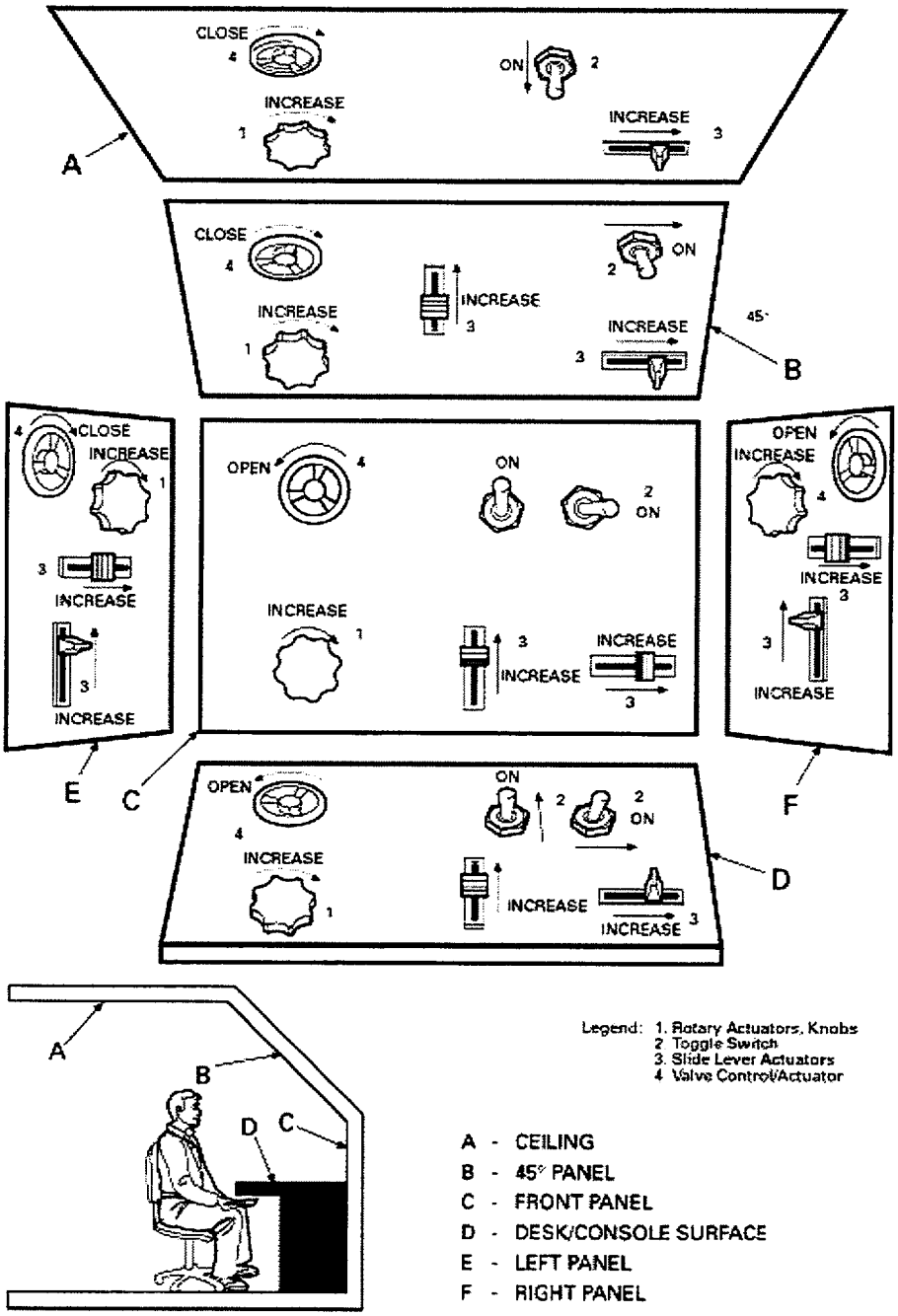


Figure 3.1 Control operation stereotypes for the U.S. population

3.1.2-1 Consistency

The coding system should be uniform throughout the control room.
Additional Information: Table 3.2 is provided as a general guideline for control coding evaluation.[0700]

3.1.2-2 Size Coding Levels

No more than three different sizes of controls should be used for discrimination by absolute size.
Additional Information: When knob diameter is used as a coding parameter, differences between diameters should be at least 0.5 inch. When knob thickness is a coding parameter, differences between thicknesses should be at least 0.4 inch.[0700]

3.1.2-3 Size Coding Uniformity

Controls used for performing the same function on different items of equipment should be the same size.[0700]

3.1.2-4 Shape Coding

When possible, controls should be differentiated by shape.
Additional Information: The shapes of conventional controls should be identifiable both visually and tactually to facilitate "blind" manipulation. When shape coding is used: (1) The coded feature should not interfere with ease of control manipulation; (2) Shapes should be identifiable by the hand regardless of the position and orientation of the control knob or handle; (3) Shapes should be tactually identifiable when gloves are worn; (4) A sufficient number of identifiable shapes should be provided to cover the expected number of controls that require tactual identification; (5) Shape-coded knobs and handles should be positively and non- reversibly attached to their shafts to preclude incorrect attachment when replacement is required; and (6) Shapes should be associated with or resemble control function, and not alternate functions.[0700, 1472]

3.1.2-5 Color Coding Contrast

The color of the control should contrast with the panel background.
Additional Information: See Table 1.3. Guidelines for color coding are given in Section 1.3.8, Color.[0700]

3.1.2-6 Color Coding Between Control and Display

When color coding is used to relate a control to its corresponding display, the same color should be used for both the control and the display.
Additional Information: Color coding should follow the recommendations of Section 1.3.8, Color.[0700]

3.1.2-7 Location Coding by Function

Controls should be located so as to be easily related to functions and functional groupings.
Additional Information: See Guideline 11.4.2-3.[0700]

3.1.2-8 Location Coding Across Panels

Controls with similar functions should be in the same location from panel to panel.
Additional Information: See Guideline 11.4.2-6.[0700]

Table 3.2 Advantages and disadvantages of various types of coding

Advantages	Type of Coding					
	Location	Shape	Size	Mode of Operation	Labeling	Color
Improves visual identification	X	X	X		X	X
Improves nonvisual identification (tactual and kinesthetic)	X	X	X	X		
Helps standardization	X	X	X	X	X	X
Aids identification under low levels of illumination and colored lighting	X	X	X	X	(when trans-illuminated)	(when trans-illuminated)
May aid in identifying control position (settings)		X		X	X	
Requires little (if any) training; is not subject to forgetting					X	

Disadvantages	Type of coding					
	Location	Shape	Size	Mode of Operation	Labeling	Color
May require extra space	X	X	X	X	X	
Affects manipulation of the use of the control (ease of use)	X	X	X	X		
Limited in number of available coding categories	X	X	X	X		X
May be less effective if operator wears gloves		X	X	X		
Controls must be viewed (i.e., must be within visual areas and with adequate illumination present)					X	X

3.2.1-1 General Keyboard Layout

An ANSI standard (QWERTY) layout should be used for the typing keyboard.
Additional Information: Common usage and the ability to transfer from one machine to another have led to the general acceptance of the QWERTY keyboard. Figure 3.2 illustrates the key arrangement.[5908]

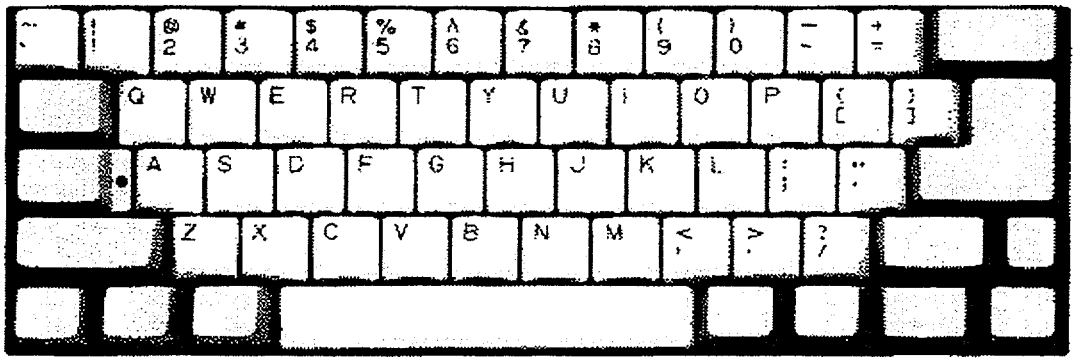


Figure 3.2 Basic QWERTY keyboard layout

3.2.1-2 Numeric Keypad

When users must enter numeric data, keyboards should be equipped with a numeric keypad.[5908]

3.2.1-3 Numeric Keypad Layout

Keypads used for numeric entry should be consistently designed.
Additional Information: Keypad layout should be one of those illustrated in Figure 3.3.[5908]

3.2.1-4 Cursor Control Capability

Horizontal and vertical cursor control keys should be provided for text processing applications.
Additional Information: Ideally, keys for cursor control should allow (1) horizontal and vertical movement, (2) movement along the diagonals, and (3) two or more rates of movement that are user selectable. Cursor keys should be dedicated to cursor movement; that is, they should not be used for any function but cursor control. If, however, the cursor keys are not dedicated (i.e., they have collateral functions) their functional status should be clearly indicated.[5908]

3.2.1-5 Cursor Key Layout

Cursor control keys should be arranged in a two-dimensional layout so that their orientation is compatible with the cursor motion they produce.
Additional Information: Cursor keys may be arranged in a "box," "cross," or "inverted-T" format. Figure 3.4 illustrates these key arrangements.[5908]

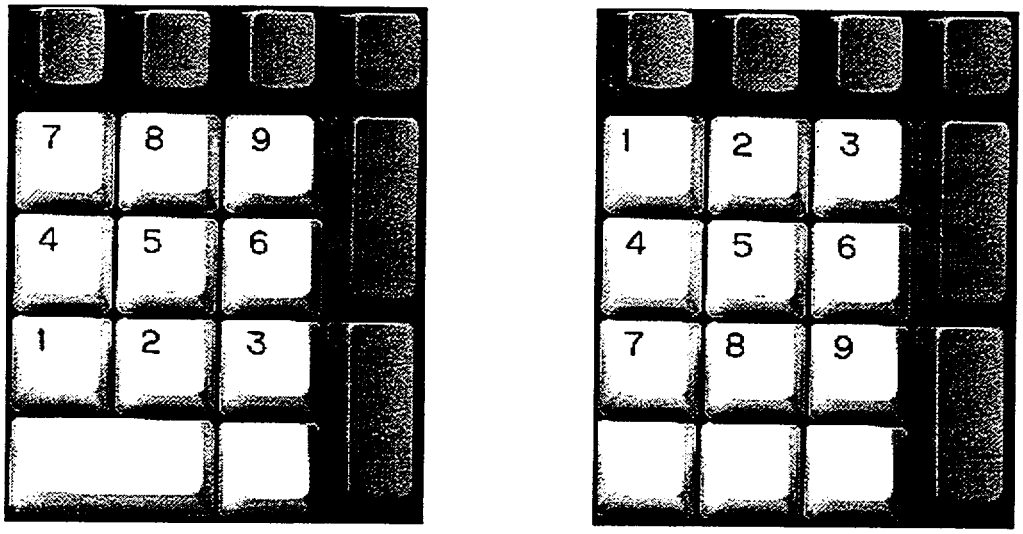


Figure 3.3 Numeric keypad layouts

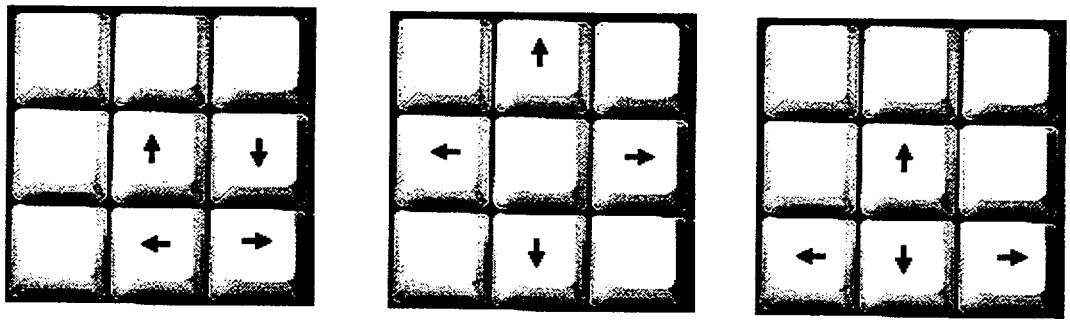


Figure 3.4 Cursor control key layouts

3.2.1-6 Overlays

Mechanical overlays, such as coverings over the keyboard, should be not used.[5908]

3.2.1-7 Keyboard Surfaces

A matte finish should be used for keyboard surfaces.

Additional Information: The spectacular reflectance (gloss) of key caps and visible surfaces should be 45 percent or less when measured with a 60-degree gloss instrument or equivalent device.[5908]

3.2.1-8 Keyboard Thickness
The thickness of the keyboard, i.e., base to the home row of keys, should be less than 2 inches (50 mm); 1.25 inches (30 mm) or less is preferred.[5908]

3.2.1-9 Keyboard Slope Adjustment
The slope of the keyboard should be adjustable by the user.
Additional Information: Keyboards should be capable of being positioned in slopes of 15 to 25 degrees from the horizontal.[5908]

3.2.1-10 Standard Keyboard Placement
The user should be able to reposition the standard keyboard on the worksurface.[5908]

3.2.1-11 Keytop Size
The minimum horizontal strike surface of the keytop should be at least 0.47 inches (12 mm) in width.
Additional Information: The keytop may be of any shape (e.g., square, round, or rectangular) provided spacing requirements are not violated.[5908]

3.2.1-12 Key Symbol Size and Contrast
The primary symbols on the keys should be a minimum of 0.1 inches (2.5 mm) in height and has a contrast ratio of 3:1.
Additional Information: Symbols on keys may be darker or lighter than the background.[5908]

3.2.1-13 Keytop Symbol Marking
Key symbols should be etched (to resist wear) and colored with high contrast lettering.
Additional Information: Keys should be labeled with a nonstylized font.[5908]

3.2.1-14 Key Spacing
Center line distances between adjacent keys should be between 0.71 and 0.75 inches (18 and 19 mm) horizontally and between 0.71 and 0.82 inches (18 and 21 mm) vertically.[5908]

3.2.1-15 Key Height
Key height for alphanumeric keyboards should be between 0.35 and 0.5 inches (10 and 13 mm).[5908]

3.2.1-16 Key Force
The maximum force required to depress keys should be between 0.9 and 5.4 ounces (0.25 and 1.5 N); a key force of between 1.8 and 2.2 ounces (0.5 and 0.6 N) is preferred.
Additional Information: The force required for key displacement should be 1.1 to 2.7 ounces (0.3 to 0.75 N) for repetitive keying tasks.[5908]

3.2.1-17 Key Displacement
Keys should have a maximum vertical displacement between 0.05 and 0.25 inches (1.5 mm and 6.0 mm); the preferred displacement is between 0.1 and 0.15 inches (2.0 and 4.0 mm).
Additional Information: Displacement variability between keys should be minimized.[5908]

3.2.1-18 Keying Feedback
The actuation of a key should be accompanied by tactile or auditory feedback or both.

Additional Information: If there is only one, tactile feedback is preferred. Should supplementary auditory feedback be used, the sound should occur at the same point in the displacement for all keys. Supplementary auditory feedback should be adjustable in volume and capable of being turned off.[5908]

3.2.1-19 Repeat Capability
A repeat capability for alphanumeric, symbol character, and cursor keys should be provided.
Additional Information: The repeat should have a user selectable delay with a default of 0.5 second. In addition, the character should be repeated at a user selectable rate with a default of 0.1 second. The physical release of the key should terminate the repeat.[5908]

3.2.1-20 Rapid Keystrokes
Rapid bursts of keystrokes should not result in characters to be lost or transmitted out of sequence.
Additional Information: Multiple-key (N-key) rollover capability reduces input errors by preserving the order in which keys are struck regardless of keys being depressed at the same time.[5908]

3.2.1-21 Keystroke Commands
When it is necessary to distinguish command entries from text input, a specially designated key should be one of the keys used for keystroke commands.[5908]

3.2.1-22 Simultaneous Keystrokes
Commands executed by chord-keying should require the user to press the keys simultaneously, not in close temporal sequence.
Additional Information: Requiring the user to press two keys simultaneously reduces the likelihood of inadvertent input of a command due to a missed keystroke that hits the specially designated key, followed immediately by another keystroke.[5908]

3.2.1-23 Inadvertent Operation
Keys with major or destructive effects should be located so that inadvertent operation is unlikely.[5908]

3.2.1-24 Alternate Key Definitions
When the keyboard is redefined, a display of the alternate characters and their locations should be available to the user.[5908]

3.2.2-1 Availability
Fixed function keys should be available to control functions that are often utilized and continuously available.
Additional Information: Lockout of fixed function keys should be minimized.[5908]

3.2.2-2 Inactive Function Keys
Unneeded function keys, either fixed or programmable, should be disabled so that no other action occurs upon their depression except an advisory message.
Additional Information: At any step in a transaction sequence, function keys that are not used for current inputs should be temporarily disabled under computer control. Mechanical overlays should not be used for this purpose.[5908]

3.2.2-3 Inactive Keys
Non-active fixed function keys should not be present on the keyboard.
Additional Information: The presence of non-relevant keys, such as those used by programmers, adds to keyboard complexity, and induces user errors. Control room keyboards should contain only those keys used by control room personnel.[5908, 0700]

3.2.2-4 Grouping
Fixed function keys should be logically grouped and placed in distinctive locations on the keyboard.
Additional Information: Color-coding can be used to highlight functional key groups. When this is done, the color of alphanumeric keys should be neutral (e.g., beige or gray).[5908]

3.2.2-5 Function Labels
Key assignments should be displayed at all times, preferably through direct marking.
Additional Information: Where abbreviations are necessary, standardized abbreviations should be used.[5908]

3.2.2-6 Consistency
Fixed function keys should be used consistently throughout the system.[5908]

3.2.2-7 Actuation
Fixed function keys should require only a single actuation to accomplish their function.[5908]

3.2.2-8 Repeat for Special Functions
Function keys (except for the delete key) should not repeat upon prolonged depression.[5908]

3.2.2-9 Status Display
When the effect of a function key varies, the status of the key should be displayed.
Additional Information: Variable function keys should be easily relabeled.[5908]

3.2.2-10 Easy Return to Initial Functions
Where the functions assigned to a set of function keys change as a result of user selection, the user should be given an easy means to return to the initial functions.[5908]

3.2.2-11 Reprogrammable or Inactive Default Functions

When keys with labeled default functions are reprogrammed or turned off, a visual indication should alert the user that the standard function is not currently accessible via that key.[5908]

3.2.2-12 Shifted Characters

Shift keys should be not required to operate variable function keys.[5908]

3.2.3-1 Dynamic Characteristics

The controller should be able to produce any combination of x-and y-axis output values.
Additional Information: The follower (cursor) manipulated by the controller should smoothly track the movement of the controller in the same direction, within +/- 10 degrees without backlash, cross-coupling, or the need for multiple corrective movements. While manipulating the control, neither backlash nor cross-coupling should be apparent to the user.[5908]

3.2.3-2 Positive Centering

If there is a "home position," the capability for an automatic return to that point should be provided.[5908]

3.2.3-3 Single Monitor/Single Controller Cursor Travel Limits

In a single monitor/single controller environment, movement of the controller should drive the follower to the edge of the screen only and not off the screen.[5908]

3.2.3-4 Separation of Selectable Screen Items

Selectable screen items or regions should be separated from each other by a sufficient distance to minimize inadvertent activation of adjacent items or regions.[5908]

3.2.3-5 Selectable Tracking Speed

The user should be able to select the controller tracking speed (control-display ratio) from a predefined range; the default speed should be moderate.
Additional Information: Control ratios and dynamic features should meet the dual requirement of rapid gross positioning and smooth, precise fine positioning. The control/display ratios should take into account both screen size and maximum maneuvering displacement. At a minimum, movement of the controller across the entire maneuvering surface should move the cursor from one side of the screen to the other.[5908]

3.2.3-6 Selectable Inter-Click Interval

If multiple clicks are required on a selection button, the user should be able to select the inter-click interval from a predefined range; the default interval should be moderate.[5908]

3.2.3-7 Limb Support for Trackballs and Mice

When trackballs and mice are used to make precise or continuous adjustments, hand, wrist, or arm supports should be provided.[5908]

3.2.3-8 Mouse Shape

The mouse should have no sharp edges but should be shaped roughly as a rectangular solid.[5908]

3.2.3-9 Use of Mouse by Either Hand

Users should be able to configure a mouse for right- or left-handed operation.[5908]

3.2.3-10 Appropriate Use of Displacement (Isotonic) Joysticks

Displacement joysticks are preferred over force joysticks when positioning accuracy is more critical than positioning speed.

Additional Information: Displacement joysticks that are used for rate control should be spring-loaded for return to center when the hand is removed. Displacement joysticks usually require less force than force joysticks and are less fatiguing for long operating periods. Hand-operated displacement joysticks may be used as mounting platforms for secondary controls, such as thumb and finger-operated switches. Operation of secondary controls is less error prone with displacement handgrips than with isometric handgrips.[5908]

3.2.3-11 Appropriate Use of Force (Isometric) Joysticks

Force joysticks are preferred over displacement joysticks when precise or continuous control in two or more related dimensions is required.

Additional Information: Force joysticks are particularly appropriate for applications: (1) which require precise return to center after each use; (2) in which feedback is primarily visual rather than tactile feedback from the control itself; and (3) where there is minimal delay and tight coupling between control and input and system reaction. When positioning speed is more critical than positioning accuracy, force joysticks should be selected over displacement joysticks.[5908]

3.2.3-12 Force Joysticks Dynamic Characteristics

The output of the force joystick should be proportional to and in the same direction as the user's perceived applied force. Maximum force for full output should not exceed 27 lb (118 N).

Additional Information: Movement should be smooth in all directions, and positioning of a follower should be attainable without noticeable backlash, cross-coupling, or need for multiple corrective movements. Control ratios, friction, and inertia should meet the dual requirements of rapid gross positioning and precise fine position. When used for generation of free-drawn graphics, the refresher rate for the follower on the display should be sufficiently high to give the appearance of a continuous track.[5908]

3.2.3-13 Displacement Joystick Dynamic Characteristics

The output of the displacement joystick should be proportional to and in the same direction as the displacement of the joystick from the center. Movement should not exceed 45 degrees from the center position.

Additional Information: The resistance should be sufficient to maintain the handle position when the hand is removed. Movement should be smooth in all directions, and positioning of a follower should be attainable without noticeable backlash, cross- coupling, or need for multiple corrective movements. Control ratios, friction, and inertia should meet the dual requirements of rapid gross positioning and precise fine positioning. When used for generation of free-drawn graphics, the refresher rate for the follower on the display should be sufficiently high to give the appearance of a continuous track.[5908]

3.2.3-14 Hand-Operated Joysticks Dimensions and Clearance

The handgrip length should be between 4.25 to 7 inches (110 to 180 mm). The grip diameter should not exceed 2 inches (50 mm). Clearances of 4 inches (100 mm) to the side and 2 inches (50 mm) to the rear should be provided to allow for hand movement.[5908]

3.2.4-1 Appropriate Use of Touch Screens

Touch screens are not recommended if the task requires holding the arm up to the screen for long periods of time.
Additional Information: Tasks involving touch screens should not require frequent, alternating use of the touch screen and keyboard.[5908]

3.2.4-2 Appropriate Use of a Light Pen

A light pen may be used for non-critical input when precise positioning is not required; it should not be used when the task would require holding the pen up to the screen for long periods of time.
Additional Information: Tasks involving light pens should not require frequent, alternating use of the light pen and the keyboard.[5908]

3.2.4-3 Appropriate Use of a Graphics Tablet

Grid and stylus devices may be used for picking data from a display and entering points on a display.
Additional Information: Displacement of the stylus from the reference position should cause a proportional displacement of the follower. The grid may be on a transparent medium allowing stylus placement directly over corresponding points on the display, or it may be displaced from the display in a convenient position for stylus manipulation. In either case, a follower should be presented on the display at the coordinate values selected by the stylus.[5908]

3.2.4-4 Activation

Light pens and graphics tablets should be equipped with an actuating/deactuation mechanism.
Additional Information: This is to prevent inadvertent actuation. For most light pen applications, a push-tip switch, requiring 2 to 5 ounces (0.5 N to 1.4 N) of force to actuate, is preferred.[5908]

3.2.4-5 Feedback

Two forms of feedback should be provided: (1) feedback concerning the position of the follower, and (2) feedback that the pointing device has actuated and the input has been received by the system.
Additional Information: Feedback can be in the form of displayed follower (such as a circle or crosshair) or highlighting.[5908]

3.2.4-6 Dynamic Characteristics

When used as a two-axis controller, movement of the pointing device in any direction on the surface of the screen or tablet should result in smooth movement of the follower in the same direction.
Additional Information: Discrete placement of the pointing device at any point on the surface should cause the follower to appear at the corresponding coordinates and to remain steady so long as the light pen is not moved. Refresh rate for the follower should be sufficiently high to ensure the appearance of continuous track.[5908]

3.2.4-7 Follower Visibility

For touch screens and light pens, the follower should be visible on screen while the pointing device is touching the screen.[5908]

3.2.4-8 Serial Command Response

The system should accept only one command at a time.[5908]

3.2.4-9 Feedback for Multiple Workstations

Discriminable audible beeps (used to supply feedback) should be used when more than one touch screen, light pen, or graphics tablet is employed.[5908]

3.2.4-10 Dimensions and Separation of Touch Zones

To allow for finger size and parallax inaccuracy, the dimensions of response areas of touch screens should be a maximum height and width of 1.5 inches (40 mm) and a minimum height and width of 0.6 inches (15 mm), with a maximum separation distance of 0.25 inches (6 mm) and minimum of 0.1 inches (3 mm).[5908]

3.2.4-11 Touch Screen Resistance

Force required to operate force-actuated touch screens should be a maximum of 5.3 ounces (1.5 N) and minimum of 0.9 ounces (0.25 N).[5908]

3.2.4-12 Neutral Tint of Touch Overlays

Touch screen overlays should have a neutral tint that does not distort colors or interfere with color coding.[5908]

3.2.4-13 Touch Screen Luminance Transmission

Touch screen displays should have sufficient luminance transmission to allow the display with touch screen installed to be clearly readable in the intended environment.[5908]

3.2.4-14 Light Pen Dimensions and Mounting

The light pen should be between 4.75 to 7 inches (120 to 180 mm) long with a diameter of 0.3 to 0.75 inches (7 to 20 mm). A conveniently located clip should be provided to hold the pen when not in use.[5908]

3.2.4-15 Graphic Tablet Size and Orientation

Transparent grids that are used as display overlays should conform to the size of the display. Grids that are displaced from the display should approximate the display size and should be mounted below the display in an orientation to preserve directional relationships to the maximum extent.
Additional Information: For example, a vertical plane passing through the north/south axis on the grid should pass through or be parallel to the north/south axis on the display.[5908]

3.3.1.1-1 Position
Pushbuttons in a row or matrix should be positioned in a logical order, or in an order related to the procedural sequence.[0700]

3.3.1.1-2 Indication of Activation
To ensure that the user knows that a pushbutton has been pressed far enough for activation, a positive indication should be provided.
Additional Information: This indication can be in the form of a snap feel, an audible click, or an integral light.[0700]

3.3.1.1-3 Pushbutton Surface
The surface of a pushbutton should offer slip resistance or be concave.[0700]

3.3.1.2-1 Dimensions of Round Pushbuttons

Round pushbuttons should conform to the dimensions given in Figure 3.5.[0700, 1472]

	Diameter (D)			Displacement (A)	
	Fingertip Operation	Thumb Operation	Palm Operation	Fingertip Operation	Thumb or Palm
Minimum	0.4 (10)*	0.75 (19)	1.6 (40)	.08 (2)	0.12 (3)
Maximum	1.0 (25)	1.0 (25)	2.8 (70)	.25 (6)	1.5 (38)

Dimensions are given in inches and (millimeters).
* Minimum diameter for guarded or recessed pushbuttons should be 0.75 inch (19mm).

Figure 3.5 Recommended dimensions for unguarded and non-recessed pushbuttons (finger- or hand-operated)

3.3.1.2-2 Resistance of Round Pushbuttons

Resistance should be 10 to 40 ounces (2.8 to 11.1 N) for fingertip operation and 10 to 80 ounces (2.8 to 22.2 N) for thumb or palm operation.[0700, 1472]

3.3.1.3-1 Discriminability

Legend pushbuttons should be readily distinguishable from legend lights.
Additional Information: This may be achieved by distinctive shape, labeling, location, or other techniques (see also Guidelines 1.6.5-7 and 1.6.5-9)[0700]

3.3.1.3-2 Legend

The legend should be readable under all environmental conditions.
Additional Information: The legend should be readable under ambient light conditions, with or without internal illumination. The illuminated condition should be clearly recognizable under the highest predicted ambient light condition and should be at least 10 percent brighter than the surrounding panel. Legend lettering and contrast should conform to recommendations for legend lights (Guidelines 1.6.5-7 and 1.6.5-8). The legend message should be specific, unambiguous, and concise. The legend message should contain no more than three lines of lettering.[0700]

3.3.1.3-3 Lamp Reliability

A lamp test or dual lamp/dual filament capability should be provided if the mean time between failure is less than 100,000 hours.[0700, 1472]

3.3.1.3-4 Easy Replacement of Covers

Lamps within the pushbutton should be replaceable from the front of the panel.[0700]

3.3.1.3-5 Safe Replacement of Lamps

Legend pushbuttons should not short out during lamp replacement or be susceptible to inadvertent activation during the process of lamp removal or replacement.[0700]

3.3.1.3-6 Correct Replacement of Covers

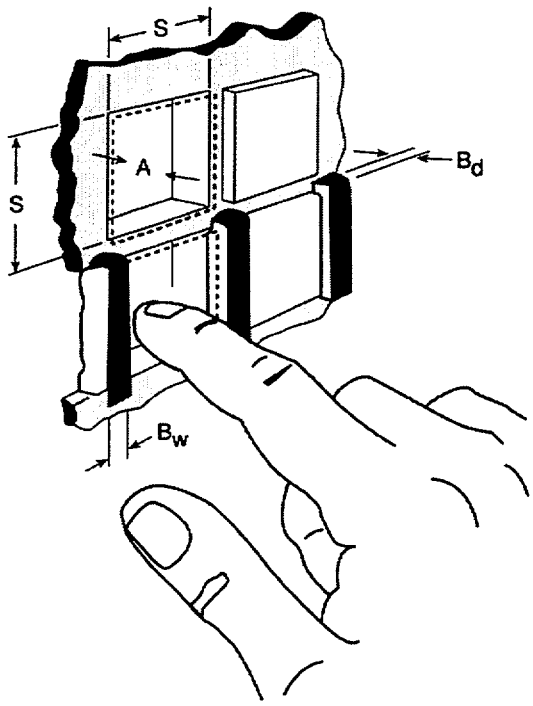
Legend covers should be keyed to prevent the possibility of interchanging the covers.[0700]

3.3.1.3-7 Barriers

Barriers should be used when legend pushbuttons are contiguous.
Additional Information: Barriers should have rounded edges.[0700]

3.3.1.3-8 Dimensions of Legend Pushbuttons

Legend pushbuttons should conform to the dimensions shown in Figure 3.6.[0700, 1472]



	Size (S)	Displacement (A)	Barriers Width (Bw)	Barriers Depth (Bd)
Minimum	0.75 (19)*	0.125 (3) **	0.125 (3)	0.188 (5)
Maximum	1.50 (38)	0.250 (6)	0.250 (6)	0.250 (6)

Dimensions are given in inches and (millimeters).
* 0.65 inches (15 mm) where switch is not depressed beyond the panel surface.
** 0.2 inches (5 mm) for switches having positive indication of activation.

Figure 3.6 Recommended dimensions for legend pushbuttons

3.3.1.3-9 Resistance of Legend Pushbuttons

Resistance should be 10 to 60 ounces (2.8 to 16.7 N).[0700, 1472]

3.3.2.1-1 Direction of Activation
Rotary control settings should increase in value with a clockwise rotation.[0700]

3.3.2.1-2 Rotary Control Shape Coding
Shape coding should be employed if rotary controls used for widely different functions are placed on the same panel.
Additional Information: General guidelines for coding controls (including shape coding) are given in Section 3.1.2, Coding of Controls.[0700]

3.3.2.1-3 Coding Specifications
Shape-coded rotary controls should be visually and tactually identifiable.[0700]

3.3.2.1-4 Rotating Knob Shape Options
Rotating knob controls for different types of control actions should be distinguishable by sight and touch and not easily confused with each other.
Additional Information: Figure 3.7 gives examples of suitable knob designs developed for three major classes of knobs, each class intended for a different purpose: multiple rotation, fractional rotation, and detent positioning. General guidelines for coding controls (including shape coding) are given in Section 3.1.2, Coding of Controls.[0700]

3.3.2.1-5 Rotary Action Control Applications
Rotary action controls should be used in situations where linear or pushbutton controls would be subject to inadvertent activation and fixed protective structures are impractical or inappropriate.[0700]

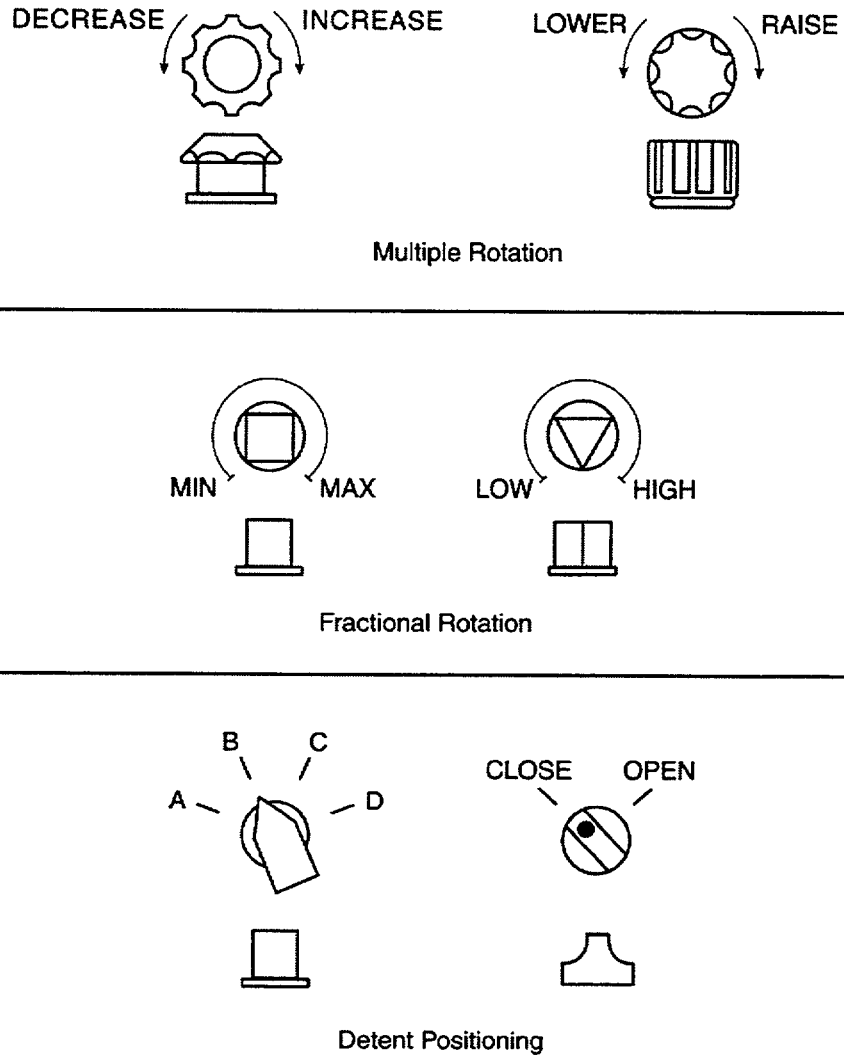
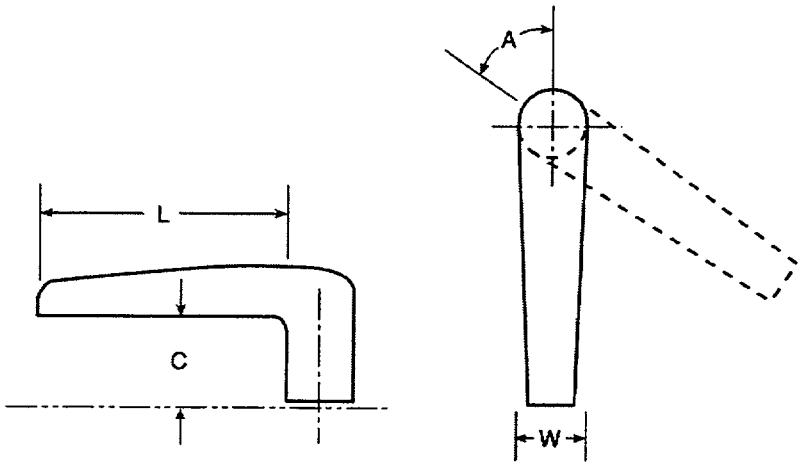


Figure 3.7 Shape-coded rotary controls

3.3.2.2-1 Dimensions of J-Handles

High torque J-handles should conform to the dimensions shown in Figure 3.8.[0700, 3659]



	Length (L)	Clearance (C)	Width (W)	Displacement (A)
Minimum	3.75 (95)	1.25 (32)	0.65 (16)	± 24°
Maximum	6.0 (150)	2.0 (50)	1.0 (25)	± 60°

Dimensions are given in inches and (millimeters).

Figure 3.8 High-torque J-handle dimensions

3.3.2.2-2 Resistance of J-Handles

Resistance should be 6 to 12 inch-pounds (0.7 to .14 N-m).[0700, 3659]

3.3.2.2-3 Low-Torque Designs

When using smaller scale J-handles, the handle portion usually has a flattened or flared tip for finger placement, and the clearance between handle and panel surface can be less.[0700]

3.3.2.3-1 Use
Key-operated controls should be used when system requirements dictate that the function being controlled should be secured against activation by unauthorized personnel.
Additional Information: If key-operated controls cannot be justified in terms of security, they are probably not necessary and should not be used. Key-operated switches should not be used solely as a means of shape coding.[0700]

3.3.2.3-2 Teeth: Single Row
Keys with a single row of teeth should be inserted into the lock with the teeth pointing up or forward.[0700]

3.3.2.3-3 Teeth: Double Row
Keys with teeth on both edges should fit the lock with either side up or forward.[0700]

3.3.2.3-4 Off Orientation
Locks should be oriented so that the OFF or SAFE state is in effect when the key is in the vertical position.[0700]

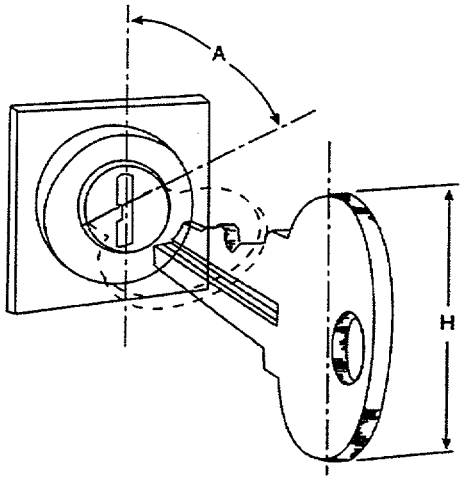
3.3.2.3-5 Key Removal
Users should not normally be able to remove the key from the lock unless the switch is turned to the OFF or SAFE position.[0700]

3.3.2.3-6 Labeling
Control positions should be labeled.[0700]

3.3.2.3-7 Actuation of Key Switch
Actuation of an item by a key operated switch should be accomplished by turning the key clockwise from the vertical OFF (i.e., upright) position.[1472]

3.3.2.3-8 Dimensions of Key-Operated Controls
Key-operated control dimensions should conform to the dimensions shown in Figure 3.9.[0700, 1472]

3.3.2.3-9 Resistance of Key-Operated Controls
The resistance of key-operated controls should be 1 to 6 inch-pounds (0.11 to 0.68 N-m).[0700, 1472]



	Displacement (A)	Height (H)
Minimum	60	0.5 (13)
Maximum	90	3.0 (75)

Dimensions are given in inches and (millimeters).

Figure 3.9 Key-operated control dimensions

3.3.2.4-1 Knobs

Knobs for continuous adjustment controls should be round in shape, with knurled or serrated edges.[0700]

3.3.2.4-2 Position Indication

When an indication of position is desirable, it should allow the user to easily recognize the position. *Additional Information:* The pointer configurations shown in bottom of Figure 3.7 may be used. Where more accuracy is required, a line should be engraved (and filled with contrasting pigment) both on top and down the side of the pointer, as shown on the knob at the bottom of the figure.[0700]

3.3.2.4-3 Knob Dimensions

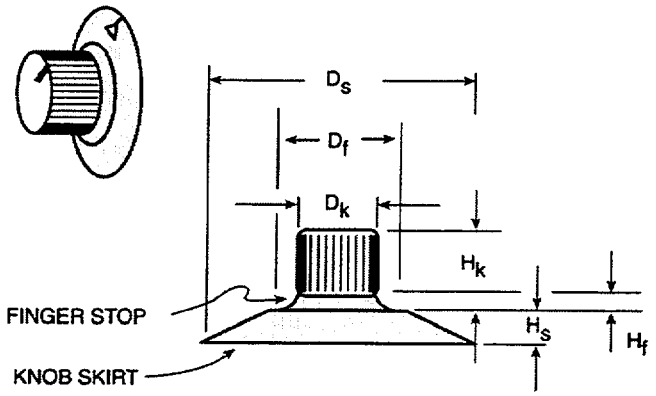
Fingertip grasp knobs should be between 0.5 and 1 inch (13 and 25 mm) in height and between 0.375 and 4 inches (10 and 100 mm) in diameter. Thumb and forefinger encircled knobs should be between 1 and 3 inches (25 and 75 mm) in diameter.[0700]

3.3.2.4-4 Knob Torque

Knob torque should be within the range of 4.5 to 6.0 inch-ounces (32 to 42 mN-m).[0700]

3.3.2.4-5 Dimensions of Knobs with Skirts

Knobs with skirts should conform to the dimensions shown in Figure 3.10.[0700]



	Knob (k)	F-Stop (f)	Skirt (s)
Diameter (D)	0.75 (19)	1.25 (32)	2.0 (50)
	Combined		
Height (H)	0.75 (19)		0.25 (6)

Dimensions are given in inches and (millimeters).

Figure 3.10 Recommended dimensions for rotary controls with finger stops and skirts

3.3.2.5-1 Selection

Rotary selector controls should be used when three or more detented positions are required, and may also be used for two-detented position operation.[0700]

3.3.2.5-2 Positioning

Detents should be provided at each control position to ensure proper positioning of a discrete rotary control.

Additional Information: It should not be possible to position a control between detented positions. To minimize the possibility of placing a rotary selector in an unused position, stops should be provided at the limits of the control range. A maximum of 24 positions should be used on a rotary selector control.[0700]

3.3.2.5-3 Readability

Rotary controls should have a moving pointer and fixed position settings to maximize readability.[0700]

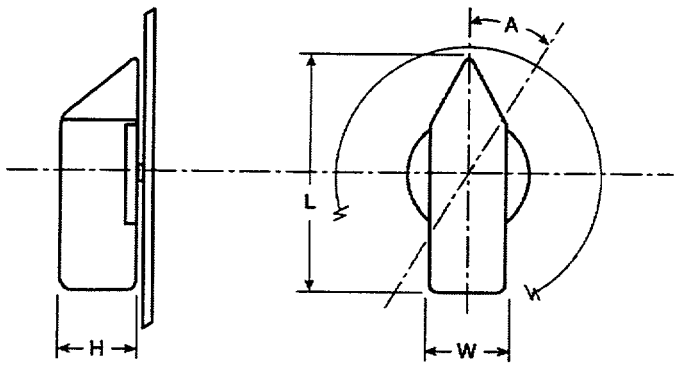
3.3.2.5-4 Position Indication

Position indication should be provided.

Additional Information: Desirable alternatives are: (1) illuminated indicator lights, (2) a line engraved both on the top of the knob and down the side, or (3) a pointer shape. It should not be possible to confuse the position of the knob in reference to position markers on the panel. To minimize the problem of parallax, pointers on knobs should be mounted close to the settings to which they point.[0700]

3.3.2.5-5 Dimensions of Rotary Selector Controls

Rotary selector controls should conform to the dimensions shown in Figure 3.11.[0700, 1472]



	Length (L)	Width (W)	Depth (H)	Displacement (A)	Displacement (A)*
Minimum	1.0 (25)		0.625 (16)	15°	30°
Maximum	4.0 (100)	1.0 (25)	3.0 (75)	40°	90°

Dimensions are given in inches a nd (millimeters).
* When special engineering requirements (such as protective clothing) or when tactually ("blind") positioned controls demand large separation.

Figure 3.11 Recommended dimensions for rotary selector switches

3.3.2.5-6 Resistance of Rotary Selector Controls

Resistance should be 1 to 6 inch-pounds (0.11 to 0.68 N-m).[0700, 1472]

3.3.2.5-7 Momentary Contact Rotary Selector Controls

Knobs for spring-loaded momentary contact rotary selector controls should be large enough to be easily held against the spring torque, without fatigue, for as long as necessary to accomplish the control action.[0700]

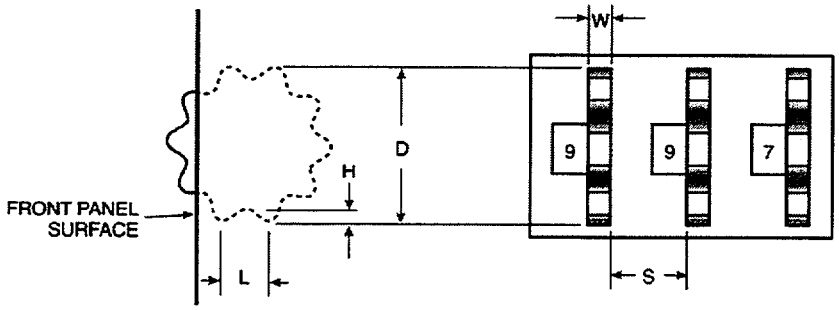
3.3.3.1-1 Visibility
To minimize error, thumbwheel readouts should be visible from the thumbwheel operating position.[0700]

3.3.3.1-2 Coding
If the thumbwheel is used as an input device, the OFF, zero, or normal position should be coded to facilitate visual recognition of status.[0700]

3.3.3.1-3 Dimensions of Continuous Adjustment Thumbwheels
At least 1 inch of circumference of a continuous adjustment thumbwheel should be exposed to permit easy manipulation.
Additional Information: A continuous adjustment thumbwheel controls moves smoothly, i.e., its motion is not 'stepped' like that of a discrete thumbwheel contol.[0700]

3.3.3.1-4 Resistance of Continuous Adjustment Thumbwheels
The resistance of a continuous adjustment thumbwheel should be between 3 and 6 ounces.
Additional Information: A continuous adjustment thumbwheel controls moves smoothly, i.e., its motion is not 'stepped' like that of a discrete thumbwheel contol.[0700]

3.3.3.1-5 Dimensions of Discrete Thumbwheel Controls
Discrete thumbwheel controls should conform to the dimensions shown in Figure 3.12.[0700, 1472]



	Diameter (D)	Trough (L)	Width (W)	Depth (H)	Separation (S)
Minimum	1.125 (30)	0.45 (11)	0.125 (3)	0.125 (3)	0.4 (10)
Maximum	3.0 (75)	.75 (19)		.25 (6)	

Dimensions are given in inches and (millimeters).

Figure 3.12 Recommended dimensions for discrete thumbwheel controls

3.3.3.1-6 Resistance of Discrete Thumbwheel Controls
The resistance of discrete thumbwheel controls should be 6 to 20 ounces (1.7 to 5.6 N).[0700, 1472]

3.3.3.2-1 Surface
The surface of slide switches should be serrated or knurled.[0700]

3.3.3.2-2 Detents
Detents should be provided for each slide switch setting.
Additional Information: Resistance should gradually increase, then drop when the switch snaps into position. The switch should not be capable of stopping between positions.[1472]

3.3.3.2-3 Accidental Actuation
Channel guards or other preventive features should be provided when accidental actuation would have undesirable consequences.[1472]

3.3.3.2-4 Orientation
Slide switches should be vertically oriented.
Additional Information: Horizontal orientation or activation slide switches should be employed only for compatibility with the controlled function or equipment location.[1472]

3.3.3.2-5 Positive Indication
Slide switches involving more than two positions should be designed to provide positive indication of the control setting, preferably a pointer located on the left side of the slide handle.[1472]

3.3.3.2-6 Dimensions of Slide Switches
Slide switches should conform to the dimensions shown in Figure 3.13.[0700]

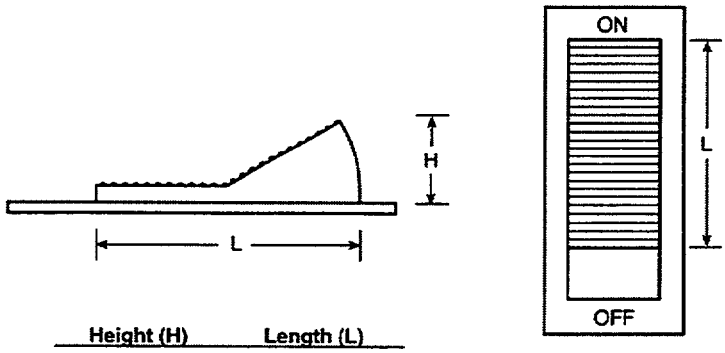


Figure 3.13 Recommended dimensions for slide switches

3.3.3.3-1 Positioning

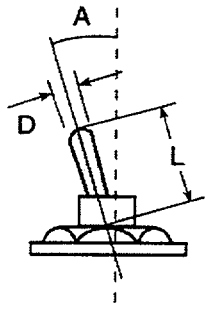
To minimize the possibility of inadvertent activation or setting between control positions, toggle switches should have an elastic resistance that increases as the control is moved and drops as the switch snaps into position.[0700]

3.3.3.3-2 Feedback

Toggle switches should emit an audible click, or provide some other source of feedback on activation.[0700]

3.3.3.3-3 Dimensions of Toggle Switches

Toggle switches should conform to the dimensions shown in Figure 3.14.[0700, 1472]



	Arm Length (L)			Displacement (A)	
	Bare Finger	Gloved Finger	Tip Diameter (D)	Two Position	Three Position
Minimum	0.5 (13)	1.5 (38)	0.125 (3)	30 °	17 °
Maximum	2.0 (50)	2.0 (50)	1.0 (25)	80 °	40 °
Desired	—		—	—	25 °

Dimensions are given in inches and (millimeters).

Figure 3.14 Recommended dimensions for toggle switches

3.3.3.3-4 Resistance of Toggle Switches

Resistance should be 10 to 16 ounces (2.8 to 4.4 N) for small switches and 10 to 40 ounces (2.8 to 11.1 N) for large switches.[0700, 1472]

3.3.3.4-1 Orientation

Rocker switches should ordinarily be oriented vertically.
Additional Information: Activation of the upper part should control the ON or INCREASE function. Horizontal orientation should be used only when required by the location of the controlled function or equipment.[0700]

3.3.3.4-2 Indication of Activation

Activation should be indicated by a snap feel, an audible click, or an integral light.
Additional Information: In the ON position, the top of the switch should be flush with the panel surface.[0700]

3.3.3.4-3 Resistance

Control resistance should gradually increase, then drop to zero when the control snaps into position.
Additional Information: This resistance should preclude the switch being placed between positions.[0700]

3.3.3.4-4 Inadvertent Activation

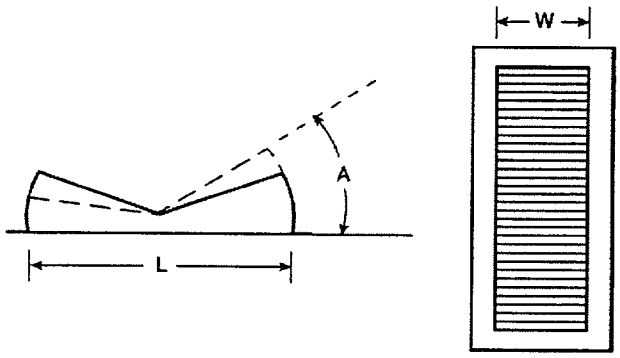
If it controls a critical function, the switch should be protected by channel guards or other means to prevent inadvertent activation.[0700]

3.3.3.4-5 Dimensions of Rocker Switches

Rocker switches should conform to the dimensions shown in Figure 3.15.[0700, 3659, 1472]

3.3.3.4-6 Resistance of Rocker Switches

Resistance should be 10 to 40 ounces (2.8 to 11.1 N).[0700, 3659, 1472]



	Width (W)	Length (L)
Minimum	0.25 (6)	0.50 (13)
Maximum	1.5 (38)	0.75 (19)

	Displacement (A)	
	Two-Position	Three-Position
Minimum	30°	18°
Optimum		25°

Figure 3.15 Recommended dimensions for rocker switches

Part II
HSI Systems

SECTION 4: ALARM SYSTEM

4 ALARM SYSTEM

Alarm systems can be described both in terms of their physical and functional characteristics. Each is discussed below. The physical characterization illustrates the relationship between the alarm system and the rest of the plant, including both equipment and operators. The functional characterization is a way of describing how the alarm system is used in the operation of the plant.

Figure 4.A shows a block diagram of a conventional alarm system. Various plant parameters (such as temperatures and pressures) are monitored by sensors (such as resistance temperature detectors and bellows pressure detectors). The output of the sensors is processed electronically to send the signals to various circuits that serve as controls, displays, and alarms. The figure shows the inputs to a parameter display and to an alarm bistable. Each alarm circuit for a parameter has a setpoint value at which the alarm is triggered. The bistable senses when the parameter exceeds the alarm setpoint; this in turn actuates the alarm display. The control room operators can then make judgments about the plant's state and what actions to take, based upon the alarm and parameter displays and the procedures. The operators would, as necessary, adjust the plant systems and components through the plant controls. Such adjustments would in turn be reflected by the sensors back into the alarms and displays.

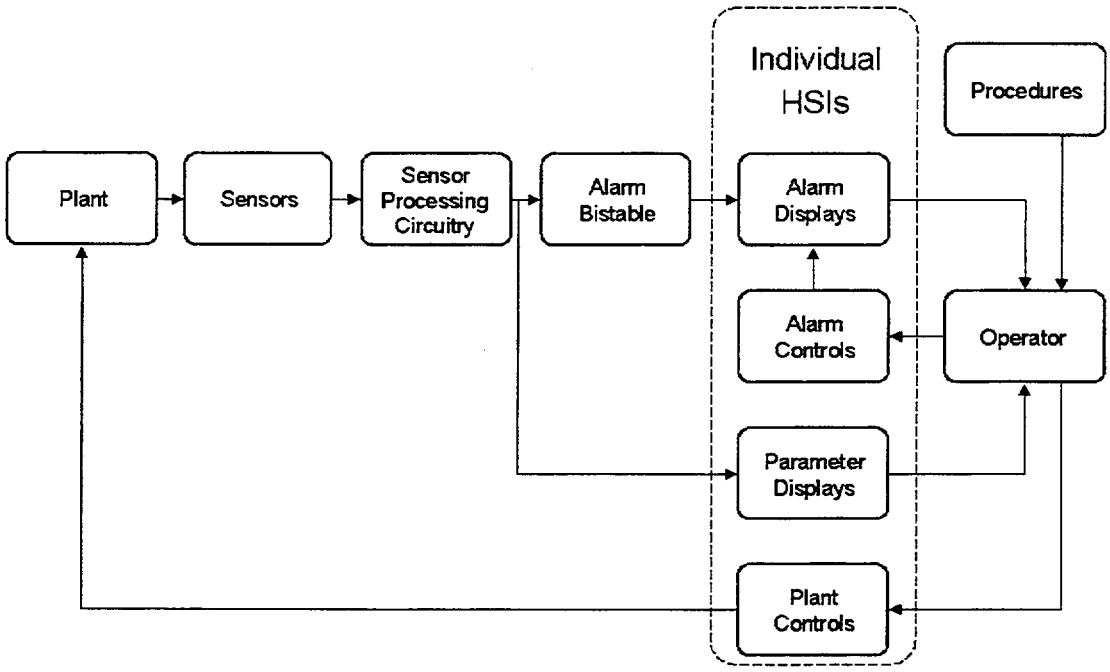


Figure 4.A Conventional alarm system

Figure 4.B presents a similar block diagram for one version of an advanced alarm system. In this version the plant, the sensors, and the sensor signal processing circuitry are similar to that for a conventional alarm system (Figure 4.A). However, the advanced alarm system (depicted in the dotted box) is typically integrated and contains a significant capability for information processing. The functioning of this circuitry is discussed later. The outputs from the advanced alarm system are typically input to some integrated HSI network that may employ VDUs or other versatile display devices. The individual parameter displays and the controls may also be included within the same integrated HSI. The operators would then use their procedures and the HSI to assess the situation, plan responses, and take any necessary actions to control the plant. Again, these actions would be reflected in a feedback loop to the plant, the sensors, and back to the HSI.

4 ALARM SYSTEM

The alarm system depicted in Figure 4.B is representative of an original analog alarm system that has had digital post-processing back-fitted to it in order to improve the alarm system's functionality. The Safety Parameter Display System (SPDS) is one example of such a digital post-processor. Other more modern alarm systems that are designed digitally from the beginning may include alarm processing at the sensor processing level.

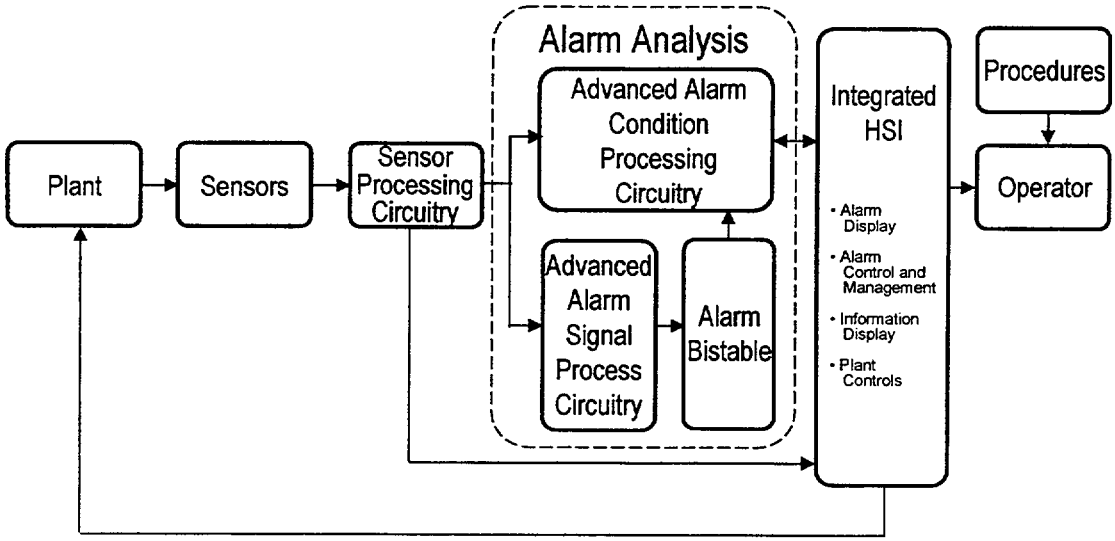


Figure 4.B Advanced alarm system

The characterization of an alarm system by the major functional and physical topics addressed in the guidance is shown in Figure 4.C. This shows the five main functions of an alarm system: Alarm definition, alarm processing, alarm prioritization, alarm display, and alarm control and management. Alarm Response Procedures (ARPs) provide more detailed information concerning the nature of the alarm condition than is typically provided in the alarm message. This characterization is useful for an HFE design reviewer, and therefore it forms the basis for organizing the alarm system guidelines. For each sub-section below, three types of information are given: an introduction to the functional area, an identification of the types of information a reviewer should address, and a reference to the appropriate section, which contains the guidelines for reviewing the topic. These alarm characteristics are discussed below.

ALARM SYSTEM FUNCTIONS

The characterization and description presented here should assist the reviewer in understanding the alarm system from a functional standpoint and guide the reviewer to appropriate guideline sections. This characterization addresses both traditional analog alarm systems and more modern systems that have significantly more capability. However, one must recognize that as alarm system designs evolve, changes in functionality may occur that affect the characterization. As an example, one trend for new advanced systems is to more completely integrate the alarm system functions into the main part of the control room interfaces, blurring the distinction between the alarms and the other displays.

The general characteristics include the basic alarm functions associated with alerting the operator, guiding the operator's actions, helping the operator monitor plant events, and facilitating the operator's interaction with the plant.

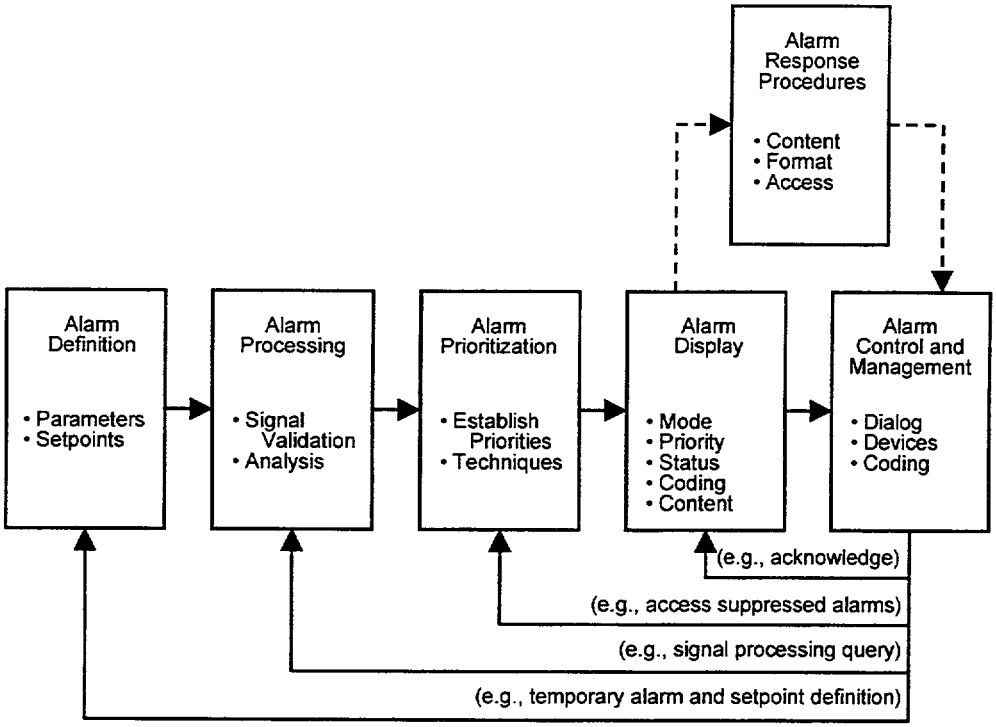


Figure 4.C Alarm system functional elements

Alarm Definition

Alarm definition is the specification of the types of process parameters to be monitored and displayed by the alarm system and the setpoints to be used to represent those parameters. The following are important considerations in alarm definition:

- Alarm categories (the events and states from which alarms are selected)
- The criteria used to select alarm parameters to represent the categories
- The criteria for determining the setpoints
- The verification process (for task appropriateness):
  - process by which alarm inclusion was checked
  - process for assuring that non-alarms are not presented in the alarm system
- Alarm states (unacknowledged, acknowledged, cleared, and reset)

The systems engineering basis for the alarm definition specification should be established to ensure that it is appropriate from a safety standpoint. Review guidelines for alarm definition are provided in Section 4.1.1.

Alarm Processing

Alarms in conventional plants tend to be stand-alone systems that alert operators to off-normal conditions and to the status of systems and components, and, by inference, the functions they support. After being alerted, the operators consult other indicators for specific information (e.g., they may determine the actual value of a parameter for which an alarm for low level had just activated). Such systems tended to

overwhelm operators during transients because of the many nearly simultaneous annunciator activations with varying degrees of relevance to the operators' tasks. Thus, alarm processing techniques were developed to support operators in coping with the volume of alarms, to identify which are significant, and to reduce the need for operators to infer plant conditions. Alarm processing addresses a fundamental aspect of system design, namely, which alarms are presented to the operating crew.

Alarm signal processing refers to the process by which signals from sensors are automatically evaluated to determine whether any of the monitored parameters have exceeded their setpoints and to determine whether any of these deviations represent true alarm conditions. Alarm signal processing includes techniques for analyzing normal signal drift and noise signals and signal validation. Normal signal drift and noise are analyzed to eliminate signals from parameters that momentarily exceed the setpoint limits but do not represent a true alarm condition. Figure 4.B illustrates the incorporation of signal processing into the circuitry for an advanced alarm system.

Signal validation is a group of techniques for comparing and analyzing redundant or functionally related sensors to identify and eliminate false signals resulting from malfunctioning instrumentation, such as a failed sensor. Alarm conditions that are not eliminated by the alarm signal processing may be evaluated further by alarm condition processing and other analyses before alarm messages are presented to the operator.

Alarm condition processing refers to the rules or algorithms used to determine the operational importance and relevance of alarm conditions; this process determines whether the alarm messages that are associated with these conditions should be presented to the operator. Figure 4.B illustrates alarm condition processing. Note that alarms screened by the alarm condition processing circuitry may or may not have already been screened by the alarm signal processing/validation circuitry. Also, the alarm condition processing circuitry receives inputs directly from the sensor processing circuitry to set the various values of logic that automatically determine how alarms are screened.

A wide variety of processing techniques have been developed; combinations of them are often employed in advanced alarm processing systems. Additionally, the processing may be occurring at various portions of the alarm systems depending on the advanced system design. The reviewer should be alert to the fact to ensure that all pertinent processing has been identified and reviewed. Each technique changes the resulting information provided to operators. For this discussion, four classes of processing techniques are defined: Nuisance Alarm Processing, Redundant Alarm Processing, Significance Processing, and Alarm Generation Processing. The classes of processing techniques are described below, and examples of each are given in Table 4.A.

Nuisance Alarm Processing – This class of processing includes techniques that eliminate alarms with no operational safety importance. For example, mode dependent processing eliminates alarms that are irrelevant to the current mode of the plant, e.g., the signal for a low pressure condition may be eliminated during modes when this condition is expected such as startup and cold shutdown, but be maintained when it is not expected, such as during normal operations.

Redundant Alarm Processing – This class of processing includes techniques that analyze for alarm conditions that are true/valid but are considered to be less important because they provide redundant information and theoretically offer no new/unique information. For example, in causal relationship processing only causes are alarmed and consequence alarms are eliminated or their priority is lowered. However, such techniques may minimize information that is used by the operator to confirm that the situation represented by the "true" alarm has occurred, for situation assessment, and for decision-making. Thus, in addition to quantitatively reducing alarms, processing methods may qualitatively affect the information given to the operating crew.

Table 4.A Alarm processing approaches

Category	Approach	Functional Description[1,2]
Nuisance	Status-alarm Separation	Separating status annunciators from alarms that require operator action.
Nuisance	Plant Mode Relationship	Alarms that are irrelevant to the current operational mode, such as start-up, are suppressed.
Redundant	Multi-setpoint Relationship	The relationship between multi-setpoints of a process variable is used to suppress lower priority alarms, e.g., when the level in the steam generator exceeds the high-high level setpoint, the high-level alarm is suppressed.
Redundant	State Relationship	Alarms associated with a well-defined situation, e.g., pump trip, are suppressed.
Redundant	Causal Relationship	The cause-effect relationship is used to identify alarms associated with causes while suppressing alarms associated with effects.
Significance	Relative Significance	Alarms associated with relatively minor disturbances during more significant events are suppressed.
Generation	Hierarchical Relationship	Using an alarm's relationship with components, trains, systems, and functions, hierarchical alarms are generated to provide operators with higher-level information.
Generation	Event Relationship	The unique pattern of alarms typically activated following the occurrence of an event is recognized and the potential initiating event is identified.
Generation	Alarm Generation	Alarms are generated when (1) conditions or events are expected to occur but do not (for example, when all control rods do not reach their fully inserted limits within a prescribed time after a scram) or (2) an alarm is expected but does not occur.

[1] For illustration purposes, the descriptions refer to alarm *suppression*, but filtering and prioritization can be also used.

[2] Functional descriptions are not intended to imply how the processing is accomplished in software.

Significance Processing – This class of processing includes techniques that analyze for alarm conditions that are true/valid but are considered to have less importance in comparison to other alarm conditions. For example, in an anticipated transient without scram event, alarms associated with minor disturbances on the secondary side of the plant could be eliminated or lowered in priority.

Alarm Generation Processing – This class of processing includes techniques that evaluate the existing alarm conditions and generate alarm messages which (1) give the operator higher level or aggregate information, (2) notify the operator when 'unexpected' alarm conditions occur, and (3) notify the operator when 'expected' alarm conditions do not occur. In effect, these processing techniques generate new (e.g., higher-level) alarm conditions. These new alarm conditions and their resulting alarm messages present an interesting paradox. Alarm systems should function to reduce errors, which often reflect the overloaded operator's incomplete processing of information. Alarm generation features may mitigate these problems by calling the operator's attention to conditions that are likely to be missed. However, the single most significant problem with alarm systems, as reported in the literature, is the large number of alarm messages presented to the operator at once. Since alarm generation creates additional messages, it may potentially exacerbate the problem.

Guidelines for reviewing alarm processing are provided in Section 4.1.2.

Alarm Prioritization

Alarm prioritization (or condition priority) refers to the determination of the relative importance to the operating crew of all current alarm conditions. This also includes consideration of alarm message availability. This assessment is accomplished in an advanced alarm system by applying alarm condition processing or in some cases processing at the sensor output level. The dimensions for evaluating the priority of an alarm condition should include the required immediacy of operator action and the significance of the condition to plant safety.

Alarm message availability refers to the process by which alarm messages are selected for presentation to the operators based on the priority of their alarm conditions. Thus, although two alarm messages may be valid for current plant conditions, one may be very important to the operator's role and should be emphasized, while the other may be of little importance and should be de-emphasized. Alarm message availability techniques emphasize important messages and de-emphasize less important ones, thereby focusing the operator's attention on the messages with the greatest operational significance.

Three alarm availability techniques have been identified – filtering, suppression, and dynamic priority coding; these techniques are defined below. (Note that these definitions are the authors'; the terms filtering and suppression are sometimes used interchangeably by other authors due to varying or imprecise definitions.)

Filtering – alarms determined by processing to be less important, irrelevant, or otherwise unnecessary are eliminated and are *not available* to the operators.

Suppression – alarms determined by processing to be less important, irrelevant, or otherwise unnecessary are not presented to the operators, but can be accessed upon request (Figure 4.D).

Dynamic priority coding – the results of alarm processing are segregated into alarms priority groupings (e.g., low and high priority) in contrast to filtering or suppressing low priority alarms determined by processing to be of lower priority.

A specific alarm system may employ a combination of these approaches. There are trade-offs among these approaches, and thus an issue remains as to which method should be used or in what contexts the various options should be exercised. Filtering completely eliminates the possibility of less important alarms distracting the operators. However, the designer may be removing information useful for other purposes. In addition, the designer must be certain that the processing method chosen is adequately validated and will function appropriately in all plant conditions. Suppression has the potential benefits of filtering by removing distracting alarms. However, since such alarms are still accessible on auxiliary displays, they potentially impose an additional secondary task workload to retrieve them. Dynamic priority coding does not conceal any information from operators. However, the method requires operators to perceptually "filter" alarms, using the priority codes, to identify the ones of higher priority. This creates the potential for distraction because it presents alarm messages of all levels of importance. The effect of these alternatives on the operators' performance needs to be considered.

The following considerations are important in prioritizing alarms:

- Specific dimensions used to prioritize the alarm's importance, e.g.,
  - Need for operator action
  - Challenges to the safety system
  - Threat to critical safety function
  - Others should be specified.
- Alarm priority characteristic
  - Number of levels for each prioritization dimension

- Method for assigning priority (for static prioritization) or computing priority (for dynamic prioritization)
- The treatment of alarms that have been removed through filtering (complete removal) or suppression (available to operators upon request).

Guidelines for reviewing alarm prioritization and availability are provided in Section 4.1.3.

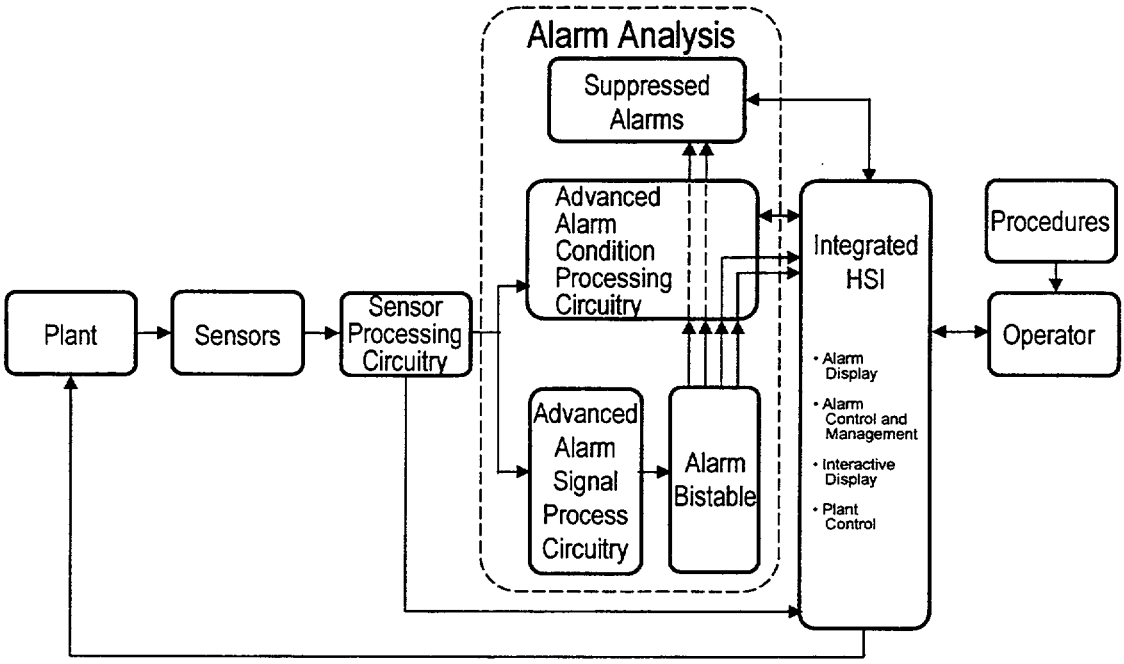


Figure 4.D Alarm suppression

ALARM DISPLAY

The information display aspects on alarms include both auditory and visual components. The auditory components are designed to capture the operator's attention to a change in the plant, while the visual components guide attention to the appropriate alarm (by using techniques such as flashing) and provide detailed alarm information (such as an alarm message).

To support the different functions of the alarm system, multiple visual display formats may be required, e.g., a combination of separate displays (such as alarm tiles) and integrated displays (such as alarms integrated into process displays). Thus, the display format of alarm information and the degree to which that information is presented separately or in an integrated fashion with other process information, are important safety considerations.

Alarm display approaches can first be characterized into three basic types:

- Spatially dedicated, continuously visible (SDCV) alarm displays (e.g., tiles).
- Alarm message lists (e.g., temporary alarm displays).
- Alarms integrated into process displays.

Other displays are possible, combining features of more than one type. For each of the alarm display types, the following characteristics are important:

- General characteristics
  - Display functions (e.g., the operators' monitoring and decision-making capabilities to be supported)
  - Degree of independence of alerting and informing functions
  - Degree of independence of priority and detailed information
  - Principles and criteria for allocating alarms to major display types
  - Alarm graphics
  - Consistency of alarm coding
- Display of high-priority alarms
- Display of alarm status
- Display of shared alarm
- Alarm messages
- Coding methods
- Detailed arrangement of alarm information
  - SDCV alarm displays
  - Alarm message lists

Guidelines for reviewing alarm displays are provided in Section 4.2. Guidelines for the review of general display characteristics are given in Section 1.

ALARM CONTROL & MANAGEMENT

The alarm control & management (or user-system interaction) aspects of the interface should be considered along two dimensions: functional requirements (what control functions are needed by operators) and implementation (how the functions are accomplished with the HSIs provided).

The typical functions used in alarm systems in the nuclear industry are silence, acknowledge, reset, and test (SART). In conventional plants, these functions are supported by dedicated controls such as pushbuttons. The SART philosophy also applies to advanced alarm systems, where interaction with the control functions may be more sophisticated and require greater flexibility than conventional alarm systems.

In addition to the basic SART controls, newer alarm systems provide many and varied alarm management functions. For example, the operator may be able to define temporary alarms, adjust setpoints, control filtering options, and sort alarms according to many separated dimensions, such as time, priority, and system. These dynamic aspects of the interface should be reviewed to ensure that excessive workload demands are avoided, while the overall functional characteristics of the alarm system are preserved. The dynamic aspects of the alarm system should not be disruptive or confusing to operators, especially when the alarm system changes modes of operation.

Some of these capabilities may require more sophisticated methods of communicating with the system than traditional dedicated switches or pushbuttons allow. The general method of communication between the operator and the alarm system, also called the dialog format, can include methods such as menu selection, command language, and special function keys (see Section 2). In advanced control rooms, this

aspect of operator communication with the system is likely to be integrated with other control room interfaces. Therefore, the alarm system may use the same input/control interfaces as the other HSI resources, such as the entry of temporary setpoints through a general-purpose keyboard.

In certain situations, such as during major process disturbances, it may be desirable to reduce workload by automating some alarm system functions, such as by silencing lower priority alarms or by temporarily stopping the flashing of an unacknowledged alarm. Similarly, automated controls may be implemented to trigger appropriate displays, such as alarm graphics, data windows, or display pages. These dynamic aspects of the alarm system should not be disruptive or confusing to operators, especially when the alarm system changes modes of operation.

Important characterization considerations for each type of user-system interaction function include the following:

- Control availability
- Modes of user interaction
  - Dialogue types (e.g., menus, command language)
  - Verification indications
  - Navigation and access of additional information
  - Additional parameter information and process displays
- Devices (design implementation)
  - Types (push buttons, switches, and touch screen)
  - Coding
  - Organization/layout (of control devices)
  - Location with respect to alarm displays and panels
- Alarm management features
  - Administrative controls
  - Operator-defined features
- Automatic features

Guidelines for reviewing alarm user-system interaction are provided in Section 4.3. Guidelines on general user-system characteristics are given in Section 2.

RELIABILITY, TEST, MAINTENANCE, AND FAILURE INDICATION

The alarm system must reliably provide alarm information to the operator. Important considerations include the reliability of the alarm system's hardware and software, the manner in which the alarm system conveys information to the operator about its failures or malfunctions, and the ease with it can be tested and maintained with minimal interruption to the operators. Each of these points is discussed below.

First, the hardware and software components of the alarm system should have sufficient reliability that the failure of a single component does not cause significant loss of functions or information. For example, the redundancy and diversity of the alarm system design should protect against alarm indications being lost or spurious alarm messages being generated as the result of sensor or signal processing malfunctions. In addition, the alarm system should allow the operators to obtain information from an alternate display if the primary display device fails.

Second, when alarm system malfunctions do occur, the alarm system should make them apparent to the operators. NPP events emphasize the importance of verifying the status of the alarm system (see, for example, Information Notice 93-47, U.S. NRC, 1993). Test controls in conventional control rooms have traditionally allowed operators to check the operation of the alarm display (e.g., detect burnt-out annunciator lamps), but not other portions of the alarm system, such as signal processing components. In addition, these controls only tested the alarm system upon demand; they did not provide continuous monitoring for anomalies. Since operators rely on the alarm system as the first indication of a process disturbance, it is important that advanced systems notify the operator of any loss of functioning. The ability of the alarm system to promptly indicate its malfunctions is an important review consideration.

Third, test and maintenance features of the alarm system should be designed so that these activities can be performed with minimal interference with the activities of the operators. Desirable design features may include built-in test capabilities, modular components that can be rapidly removed and replaced, and rear access panels which prevent maintenance activities from obstructing the operator's view of controls and displays.

Guidelines for reviewing these characteristics are provided in Section 4.4.

ALARM RESPONSE PROCEDURES

Alarm Response Procedures (ARPs) provide more detailed information concerning the nature of the alarm condition than is typically provided in the alarm message. Typically, the information provided is alarm source (sensor), setpoint, causes, automatic actions, and operator actions. This information is especially important to operators when an unfamiliar alarm is activated or when an alarm seems inconsistent with the operator's understanding of the state of the plant. ARPs may be hardcopy or computer-based documents.

The following characteristics of ARPs are important:

- ARP information content
- ARP format
- ARP location
- Methods of user access to, and interaction with, ARPs (especially computer-based ARPs)

Guidelines for reviewing ARPs are provided in Section 4.5.

CONTROL-DISPLAY INTEGRATION AND LAYOUT

Control-display relationships and general layout significantly impact the operator's performance with alarm systems, as they do for other aspects of the HSI. The following considerations are important:

- Control console layout of alarm display devices and controls
- Alarm display layouts for VDUs
- Relationship between alarm controls and displays and the associated process indicators and controls
- Physical relationship between the operators and the alarm controls and displays and the associated process indicators and controls

Guidelines for reviewing control-display integration are provided in Section 4. 6.

INTEGRATION WITH OTHER HSI ELEMENTS

The consistency and compatibility of the alarm system with the rest of the HSI can affect the operator's performance and, therefore, should be addressed. Guidelines for reviewing control-display integration are provided in Section 4.7.

4 ALARM SYSTEM
4.1 Alarm System High-Level Functions
4.1.1 Alarm Definition

4.1.1-1 Alarm Selection
The following criteria should be included in the basis for selecting alarm conditions:

- Monitoring critical safety functions and key parameters,
- Preventing personnel hazards,
- Avoiding significant damage to equipment having a safety function,
- Assuring that technical specifications are met,
- Monitoring emergency procedure decision points, and
- Monitoring plant conditions appropriate to plant modes ranging from full power to shutdown.

Additional Information: One of the key aspects of an alarm system is to help ensure that the plant remains within the safe operating envelope as defined by the Safety Analysis Report (SAR) and technical specifications. This includes ensuring that automatic systems can still perform their intended functions to protect the plant and personnel. This assurance can be provided in a number of ways by the alarm system with the monitoring of critical safety functions and key parameters being a typical choice. Selection of alarms should consider all operational modes including shutdown. After a scheme for selecting alarm conditions has been developed and applied, the selected alarm conditions should be reviewed to verify that important aspects of all of the above categories are addressed within the main control room alarm system.[6105, 6684, 0700]

4.1.1-2 Timely Warning
Alarm set points should be determined to ensure that the operating crew can monitor and take appropriate action for each category of alarms, e.g., respond to out-of-tolerance conditions, in a timely manner.
Additional Information: Alarms are established to help ensure that the plant remains within SAR and technical specification limits. In order to achieve this, the setpoints may be specified at conservative levels that are well within the actual limits to allow sufficient response time for operators and plant systems. Thus, where practical, alarm setpoints should be determined such that the operator is alerted before a major system or component problem results in a condition which causes a loss of availability (e.g., plant trip), equipment damage, violation of SAR and technical specification requirements, or other serious consequences. Other criteria are acceptable if they do not compromise these factors.[6105, 0700]

4.1.1-3 Setpoint Determination and Nuisance Alarm Avoidance
The determination of alarm setpoints should consider the trade-off between the timely alerting of an operator to off-normal conditions and the creation of nuisance alarms caused by establishing setpoints so close to the "normal" operating values that occasional excursions of no real consequence are to be expected.
Additional Information: When determining setpoints, consideration should be given to the performance of the overall human-machine system (i.e., operator and alarm system acting together to detect process disturbances). If setpoints are established such that many false alarms occur, operators become less likely to respond to the alarm, especially when their tasks become cognitively demanding. Processing techniques (see Guideline 4.1.2-4) are applied to prevent normal variation from producing alarms. Under some circumstances, however, preventing such alarms may deprive operators of needed information. In cases where raising an alarm's setpoint or delaying its presentation is not acceptable, more sophisticated techniques (e.g., alarms based on rate of change of the parameter or the time at which the parameter is projected to exceed a setpoint) should be considered.[6105, 6684, 0700]

4.1.1-4 Darkboard Configuration

Alarms and setpoints should be designed so that only parameters and conditions that fall outside of the normal and expected range and that require operator attention or action are in the alarm state.

Additional Information: This has traditionally been referred to as the darkboard concept and is applicable when at full power operation. In practice it may be difficult in some plants to completely achieve a darkboard but that should be the goal. If the alarm system does not have this capability for all operating conditions, it should be in effect when all systems are lined up in their most typical configuration for full-power operation.

This concept has implications for the plant's operating philosophy as well, including issues such as (1) repairing failed equipment expeditiously, (2) taking corrective actions for instrument drifts that cause alarms, and (3) correcting conditions that frequently lead to repeat alarms.[0700, 6105]

4 ALARM SYSTEM
4.1 Alarm System High-Level Functions
4.1.2 Alarm Processing

4.1.2-1 Assured Functionality Under High Alarm Conditions
The alarm processing system should ensure that alarms that require immediate action or indicate a threat to plant critical safety functions are presented in a manner that supports rapid detection and understanding under all alarm loading conditions.
Additional Information: Alarm processing should be provided to ensure that alarm functional criteria are not lost under any operational or accident conditions. The alarm system should provide the capability to reduce the number of concurrent alarm messages so that during off-normal conditions, the alarm system does not overload of the operator's cognitive processes. Special attention should be given to the problem of detecting subsequent malfunctions following the presentation of alarms related to an initial disturbance.[6105, 6684]

4.1.2-2 Alarm Reduction
The number of alarm messages presented to the crew during off-normal conditions should be reduced by alarm processing techniques (from a no-processing baseline) to support the crew's ability to detect, understand, and act upon all alarms that are important to the plant condition within the necessary time.
Additional Information: Since there is no specific guidance on the degree of alarm reduction required to support operator performance, the designer should evaluate the system with operators to assess the effectiveness of the alarm reduction process. This assessment should include evaluations that simulate the operation of the alarm system under situations that activate multiple alarm conditions and/or generate increased operator workload. The use of dynamic mockups and prototypes of the alarm system and dynamic control room simulators should be considered when developing these assessments.[6105, 6684]

4.1.2-3 Alarm Signal Validation
Sensor and other input signals should be validated to ensure that spurious alarms are not presented to plant personnel, due to sensor or processing system failure.
Additional Information: Instrumentation failure is not a common problem in NPPs. However, when such failures occur such as a failed sensor, biased or false signals are generated. The use of these signals by the alarm system may result in the presentation of either false or nuisance alarm messages. Such alarm messages are misleading and may interfere with the crew's situation assessment or reduce the crew's confidence in future alarm messages. Signal validation is a set of alarm processing techniques by which signals from redundant or functionally related sensors are compared and analyzed to determine whether a true alarm condition exists. The purpose of these techniques is to prevent the presentation of false alarms to the operator due to malfunctioning plant instrumentation. Hence, signal validation should be included in an advanced alarm system.[6105]

4.1.2-4 Parameter Stability Processing
The alarm system should incorporate the capability to apply time filtering, time delay, or deadbanding to the alarm inputs to allow filtering of noise signals and to eliminate unneeded momentary alarms.
Additional Information: Noise from plant instrumentation may result in signals that momentarily exceed the limit for alarm message activation for a plant parameter. Time delay processing prevents this signal from generating a spurious alarm message to the crew. In some cases, applying these techniques may reduce the timeliness of the information provided to operators. When this tradeoff is not acceptable, other processing methods can be used (see additional information for Guideline 4.1.1-3).[6105, 6684]

4.1.2-5 Segregation of Status Indications

Status indications, messages that indicate the status of plant systems but are not intended to alert the user to the need to take action, generally should not be presented via the alarm system display because they increase the demands on the users for reading and evaluating alarm system messages.
Additional Information: While status information is important to operators, status indications are not alarms and should be presented to operators via a non-alarm display, e.g., on process displays. If the presentation in the alarm display of status indications is justified on the basis of the unique aspects of the design, such status messages should be designed so that operators may readily distinguish them from true alarm messages.[6105, 6684]

4.1.2-6 First-Out Processing

As an aid to diagnostic procedures and root cause analysis, provision should be made for identifying the initiating event associated with automatic plant trips through the use of first-out alarms.
Additional Information: In most conventional alarm systems used in nuclear power plants, first-out alarms, which identified the parameter within an interrelated group that first exceeded its setpoint, were provided to support operators in determining the initiating cause of a reactor or turbine trip. Advanced alarm systems should include this first-out capability along with the results of any additional processing that could improve the identification of the initiating event. First-out alarms work well where all signals respond equally quickly (e.g. electrical 'sequence of events' monitoring), but are not necessarily as useful to operators where response characteristics can be time-variable. This situation arises in process systems because of differential lags in some measurements (e.g. temperature, level) compared to others (e.g. pressure, electrical parameters).[6105, 0700]

4.1.2-7 Mode Dependence Processing

If a component's status or parameter value represents a fault in some plant modes and not others, it should be alarmed only in the appropriate modes.
Additional Information: The following is an example of mode dependent processing. The fact that a particular pump has shutdown may only have operational significance to the crew when the plant is operating in the power range. Mode dependent processing would allow this alarm message to be presented when the plant is in the power range but not when it is in other modes (e.g., hot standby). Strategies have also been described in which different alarm setpoints are in effect for some parameters depending on plant mode. When there may be mode-dependent changes in the alarm system's responses the cautions contained in Guideline 4.3.6-3 should be considered.[6105, 6684]

4.1.2-8 System Configuration Processing

If a component's status or parameter value represents a fault in some system configurations and not others, it should be alarmed only in the appropriate configurations.
Additional Information: The following is an example of system configuration processing. The fact that a particular pump has a low discharge pressure may indicate that the pump is not running or it might only indicate a fault when the associated fluid system is configured to perform a particular function. Other discharge pressures may be appropriate when the fluid system is configured to perform a different function. In addition, a low pump discharge pressure may not be relevant when the fluid system is taken out of service. System configuration processing would allow the alarm message for pump discharge pressure to be presented when the fluid system is in the proper configuration and prevent its presentation when the system is in an alternate configuration.[6105, 6684]

4.1.2-9 Logical Consequences Processing

If a single event invariably leads to subsequent alarmed events that are the direct consequence of this event, only the alarm message associated with the main event may be presented and the other alarm messages suppressed, so long as this does not interfere with the use of alarm information.
Additional Information: For example, logical consequences processing may be used to suppress alarms that follow as a logical consequence of trip or isolation conditions. When implementing logical consequences processing, the designer should ensure that messages associated with the "consequence" alarm conditions are not needed for other operational tasks, and that operators are aware that the associated "consequence" alarm conditions were generated but not presented. This guideline only suggests suppression of these alarms, not their complete elimination (i.e., filtering).[6105, 6684]

4.1.2-10 Exceptions to Expected Alarm Patterns

The system should notify the user when 'unexpected' alarms occur, if the alarm processing logic can support such an analysis.
Additional Information: A related feature that may also be considered is to annunciate the absence of expected alarm patterns; i.e., the system can notify the operator when 'expected' alarms do not occur, if the alarm processing logic can support such an analysis. Such analyses may apply, for example, during certain transients (e.g., reactor scram) where the expected alarm pattern is well known.[6105]

4.1.2-11 Intelligibility of Processed Alarm Information

The alarm system should provide functions that enable users to evaluate the meaning or validity of the alarm messages resulting from alarm processing; for example, it should be possible to view the inputs to the alarm processing system.
Additional Information: Complexity of the processing impacts the operator's ability, as the system supervisor, to understand the results of alarm processing and its constraints and limitations. Since the alarm system is the operator's first indication of process disturbances and operators will confirm the validity of alarm signals prior to taking action, it is essential that operators easily comprehend the meaning of alarm data, how they are processed, and the bounds and limitations of the system. An alarm system that combines multiple processing methods should not be so complex that it cannot be readily understood and interpreted by the operators who must rely on the system's outputs. If operators are unaware of the relationships among displayed alarms and how those relationships might depend on the processing being applied, they may draw incorrect conclusions about the state of the system or the reliability of the alarms. For example, operators may need to view sensor data and values that result from alarm system processing under certain circumstances, such as if the pattern of alarm messages appears to be contradictory, or if operators suspect that there is a problem with the processing system such that the results of alarm processing are incorrect.[6105, 6684]

4.1.3-1 Prioritization Criteria

Alarm messages should be presented in prioritized form to indicate urgency (immediacy of required action) and challenges to plant safety.

Additional Information: Additional alarm priority dimensions, such as challenges to plant productivity or investment protection, may also be implemented. The selected prioritization scheme should be logical such that those alarms of the highest safety significance receive the highest priority and such that the prioritization appears reasonable to operators.[6105, 6684, 0700]

4.1.3-2 Access to Suppressed Alarms

When alarm suppression is used, the user should be able to access the alarm information that is not displayed.

Additional Information: Suppressed alarms are not presented to the operators, but they can be accessed by operators upon request. The method for accessing suppressed alarms and the scheme for their presentation to the operators should not be excessively complex.[6105, 6684]

4.1.3-3 Filtered Alarms

Alarm filtering should only be employed where alarm messages have no current operational significance to the crew's monitoring, diagnosis, decision making, procedure execution, and alarm response activities.

Additional Information: As the term is used here, filtered (as contrasted with suppressed) alarm messages are eliminated and are not available to the operators. Research has indicated that operators prefer to have information available to them to support verification and decision-making activities. Thus, only alarms that can be demonstrated to have no operational significance to operators should be filtered. This includes alarm messages that are irrelevant within the context of the current plant mode or the configuration of the associated plant system. For example, alarm messages that indicate that a pump discharge pressure is low after the fluid system has been removed from service should be filtered. Alarms that are considered redundant or lower priority should be suppressed (where operators can retrieve them) rather than filtered.[6105, 6684]

4.2.1-1 Display Functions

The alarm display should support the user's ability to rapidly discern:

- Priority (e.g., urgency for action and importance to plant safety);
- Distinct alarm states: new, acknowledged, and cleared;
- The first-out alarms for reactor trip;
- The need to access other displays to verify or clarify the alarm state; and
- The difference between alarms which can be cleared through ongoing corrective actions (i.e., by operations personnel) and alarms that require significant maintenance intervention.

Additional Information: Multiple alarm display formats, such as dedicated tile-like display and message lists, may be necessary to satisfy all alarm information needs.[0700, 6105, 6684]

4.2.1-2 Coordination of Alarm Alerting and Informing Functions

When alarm alerts are displayed separately from detailed alarm information, the design should support rapid transitions between alerts and detailed information.

Additional Information: In conventional annunciator tile-based alarm systems, the annunciator tile performs both the alerting function (i.e., providing a salient indication of the presence of an alarm condition) and the informing function (i.e., providing information that describes the nature of the alarm condition). In advanced alarm systems, the alerting and informing functions may be separated. For example, an alarm tile display may alert the operator to the presence of an alarm condition while an alarm message list display may provide detailed information such as the alarm parameter name and setpoint value. The presentation of the alerting and informing information should be coordinated so the operator can rapidly access detailed alarm information associated with the alarm condition alerts.[6105, 6684]

4.2.1-3 Presentation of Alarm Priority with Detailed Alarm Information

When alarm alerts are displayed separately from detailed alarm information, the detailed alarm information display should provide an indication of the priority and status of the alarm condition.

Additional Information: The operational significance of the detailed alarm information, such as the parameter name and the exceeded setpoint value, may be more readily apparent to the operator when accompanied by an indication of alarm's priority and its status (e.g., whether it is acknowledged or unacknowledged).[6105, 6684]

4.2.1-4 Use of Spatially Dedicated, Continuously Visible Displays

Spatially dedicated, continuously visible (SDCV) alarm displays should be considered for:

- Regulatory Guide 1.97 Category 1 parameters,
- Alarms that require short-term response,
- The most important alarms used in diagnosing and responding to plant upsets, and
- The most important alarms used to maintain an overview of plant and system status.

Additional Information: Spatial dedication means that the alarm messages always appear in the same position. Continuously visible means a parallel presentation method is used, i.e., the alarm information is always available to the operator, as opposed to serial presentation methods in which the operator must select the information to be seen. A SDCV alarm display (such as is provided by conventional tiles) generally has been found during high-density alarm conditions to be superior to other forms of alarm presentation, such as message lists. SDCV displays provide perceptual advantages of rapid detection and enhanced pattern recognition.[6105, 6684]

4.2.1-5 Alarm Coding Consistency

Coding (e.g., flash-rate, intensity, and color coding) conventions should be consistently applied throughout alarm displays (e.g., on tiles and on VDUs).[6105]

4.2.1-6 Multi-Unit Alarms

Alarms for any shared systems in multiple-unit plants should be duplicated in all control rooms.
Additional Information: Multiple-unit NPPs may contain systems that are shared by two or more units. The status of any such equipment should be provided in all control rooms. When an item of shared equipment is being operated from one control room, a status display or signal should be provided in all other control rooms where the condition of the equipment is operationally relevant (e.g., other locations from which the equipment could be controlled).[0700]

4.2.2-1 Precedence for Important Information

Alarms that have higher importance or greater safety significance should be given greater priority in their presentation than less important or significant alarms.

Additional Information: The priority of presentation should be part of an overall process for alarm management, which may include coding for the level of importance or priority, and alarm processing, filtering, and suppression.[6105]

4.2.2-2 Simultaneous Display of High-Priority Alarms

For non-spatially dedicated alarm presentations such as VDU message lists, sufficient display area should be provided for the simultaneous viewing of all high-priority alarms.

Additional Information: Non-spatially dedicated alarm displays, such as message lists, should generally not be used as the primary method of presenting high-priority alarm messages. If non-spatially dedicated alarm displays are used, they should have sufficient display space available for simultaneous presentation of all high-priority alarms under the worst credible conditions. Operators should never have to page or scroll a display to view high-priority alarms.[6105, 6684]

4.2.2-3 Coding of Alarm Priority

A method of coding the visual signals for priority should be employed.

Additional Information: Acceptable methods for priority coding include color, position, shape, and special symbols. Color and position (top to bottom) are especially effective visual coding methods.[6105]

4.2.3-1 Indication of Alarm Status

Unacknowledged, acknowledged, and cleared alarm states should have unique presentations to support the users' ability to rapidly distinguish them.[6105]

4.2.3-2 Unacknowledged Alarm Indication

Unacknowledged alarms should be indicated both by visual (e.g., flashing) and audible means.
Additional Information: When unacknowledged alarm messages are presented on a VDU, the message text itself should not flash. Rather, an adjacent flashing symbol should be used to indicate the unacknowledged message (see Guideline 1.3.10-10, Flash Coding for Text).[6105, 6684]

4.2.3-3 Notice of Undisplayed Unacknowledged Alarms

If the user is not currently viewing the VDU display where unacknowledged alarm messages appear, the alarm system should notify the user that an alarm message is available, the priority of the alarm message, and the location where the alarm message can be found.[6105]

4.2.3-4 Acknowledged Alarm Indication

After the user has acknowledged an alarm (e.g., pressed the acknowledge button), the alarm display should change to a visually distinct acknowledged state.[6105]

4.2.3-5 Clearing Alarm Ringback

When an alarm clears (i.e., the parameter returns to the normal range from an abnormal range), the return to normal conditions should be indicated by visual and audible means.
Additional Information: Ringback, alerting the operator when a parameter returns to normal, should not be required for all alarms but should be required when it is important that the operator know immediately when the deviation has cleared, or when the deviation is not expected to clear for some time. Such cleared alarms should provide a positive indication by initiating audible and visual signals. Techniques that may be employed include: a special flash rate (one-half the normal flash rate is preferred, to allow discrimination); reduced brightness; or a special color. Cleared alarms should have a dedicated, distinctive audible signal, which should be of finite and relatively short duration.[6105, 0700]

4.2.3-6 Cleared Alarms That Re-Enter the Abnormal Range

If an alarm has cleared but was not reset and the variable re-enters the abnormal range, then the condition should be presented as a new alarm.
Additional Information: When an alarm clears, the operator is informed via the ringback feature that the value is now in its normal range. Since the operator might expect the parameter to remain in the normal range, the alarm system should alert the operator when the parameter deviates from the normal range. If the variable again enters the abnormal range, the alarm system should behave as it does for new alarms, by producing visual and auditory signals to alert the operator. For cases in which a variable might move (e.g., oscillate) in and out of the normal range, alarm processing should be used to prevent the frequent reoccurrence of the alarm from becoming distracting to the operator. One technique might be to require the parameter to move further into the normal range before the alarm clears. Another technique might be to require the parameter to remain within the normal range for a particular amount of time before allowing the alarm to clear.[6684]

4.2.4-1 Minimize Shared Alarms

Alarms that are triggered by any one of an aggregate of individual alarms (e.g., 'Pump Trouble') and which require the operators to perform additional actions to determine the cause should be limited. *Additional Information:* This guideline does not apply to the use of alarm processing through which individual alarms are logically processed to provide more operationally meaningful, higher-level alarm messages. By contrast, shared alarms are defined by the activation of one or more of a set of different process deviations. For example, a "trouble" message may combine several potential problems associated with a single plant system or component, or it may address the same problem for a group of similar components (e.g., a bearing temperature alarm may address bearings from more than one component). When shared alarms are used, an inquiry capability should be provided to allow the operator to obtain specific information about which of the ganged parameters exceeded its setpoint. Criteria for the use/avoidance of shared alarms are given in Table 4.1. In traditional (i.e., tile-based annunciator) alarm systems, shared alarms imposed additional workload on the operator compared to single alarms because the operator had to identify the deviant parameter(s). This type of shared alarm should be minimized in advanced alarm systems. Some advanced alarm systems automatically present information related to the deviant parameter when the shared alarm is initiated. This reduces the operator workload associated with retrieving alarm information and minimizes the negative effects of shared alarms.[6105, 6684, 0700]

Table 4.1 Shared alarm considerations

TYPES OF ALARMS THAT MAY BE CONSIDERED FOR COMBINATION (SUBJECT TO THE RESTRICTIONS LISTED BELOW)
• Alarms for the same condition on redundant components, or logic trains, when each has a separate indicator and the indicators are placed in close proximity on the console (e.g., pump A or B trip, logic train A or B actuation)
• Alarms for several conditions relating to one component or several redundant components, which require the operator to obtain further diagnostic information either by sending an auxiliary operator out to the component(s) or checking the computer (e.g., pump A or B trouble)
• Alarms for several conditions that call for the same corrective action
• Alarms that summarize single-input alarms elsewhere in the control room
CONDITIONS UNDER WHICH ALARMS SHOULD NOT BE COMBINED
• Different actions are to be taken depending on which alarm condition exists and information is not readily available to the operator to identify which constituent is alarming
• Information or protection for other alarm constituents is not available to the operator after any one alarm constituent has activated the combined alarm (reflash can provide such protection as discussed in Guideline 4.2.4-3)
• The constituent conditions are not of the same importance

4.2.4-2 Access to Shared Alarm Information

The system should allow users to access the individual alarm information when a shared alarm activates.
Additional Information: The information could be provided by means of alarm messages on a VDU, an alarm list on an alarm printer, or by other means. This information may be provided automatically or by operator action.[0700]

4.2.4-3 Shared Alarm Reflash

If a new parameter deviation has occurred before a preceding alarm has cleared, the shared alarm should return to the new alarm state (e.g., flashing).
Additional Information: The alarm logic system should provide the capability to "reflash" (i.e., reactivate the visual and audible alert indications for the alarm) when subsequent alarm conditions occur after the initial alarm condition has been acknowledged.[6105, 0700]

4.2.5-1 Alarm Titles/Legends

Titles/legends should be clearly understandable, use standard terminology, and address conditions specifically.
Additional Information: For example, specifically identify the parameter and state (e.g., HIGH PRESSURE) instead of using one legend for multiple parameters or multiple states (e.g., TEMPERATURE-PRESSURE or HIGH-LOW).[0700]

4.2.5-2 Alarm Messages – SDCV Tile Format

The format of messages on alarm tiles or tile-like displays should be consistent for all alarms.
Additional Information: Information on a tile might be organized as follows: top line, name of alarmed parameter; middle line, alarm setpoint value; bottom line, indication of severity.[6105]

4.2.5-3 Alarm Messages – List or Printer Format

The format of printed alarm lists should be consistent with that of VDU and SDCV displays.[6105]

4.2.5-4 Alarm Source

The content of each message should provide information that identifies the alarm source.
Additional Information: Information should be available as to which specific sensor (or group of sensors) supplied the alarm signal.[6105]

4.2.5-5 Alarm Priority

An alarm message should indicate its priority.[6105]

4.2.5-6 Setpoint Values

If an alarm condition requires verification before action is taken, the relevant setpoint limits should be included in the alarm message when alarm information is presented on a VDU or is printed.[6105]

4.2.5-7 Parameter Values

Deviant parameter values should be included in the alarm message when alarm information is presented on VDU or printer displays.[6105]

4.2.5-8 Required Immediate Actions

Immediate actions should be presented or made available directly upon request when alarm information is presented on VDU or printer displays.
Additional Information: To support the general alarm system function of guiding the operator's response to an alarm, the immediate actions should be provided to the operator. For conventional alarm systems, the immediate operator actions should be available in Alarm Response Procedures that are clearly and simply keyed to an alarm tile and located nearby for easy and quick reference. In this case, the procedure would contain those items that could not be incorporated into the alarm display itself (e.g., alarm source, setpoint value, immediate actions, and follow-up actions). Advanced alarm systems may present the relevant alarm response procedure (e.g., via a nearby VDU).[6105]

4.2.5-9 Reference to Procedures

When alarm information is presented on VDU or printer displays, references to alarm response procedures should be provided.

Additional Information: The document title, major section, and page number should be included in such references.[6105]

4.2.5-10 Reference to Other Panels

Alarms which refer the user to another, more detailed display located outside the main operating area should be minimized.

Additional Information: Advanced alarm systems should be designed such that required information is readily accessible from within the main operating area.[0700]

4.2.6.1-1 Coding Effectiveness

The coding scheme used by the alarm system should assure rapid detection and interpretation by the users under all control room operating conditions.[0700]

4.2.6.1-2 Coding Dimension Discriminability

Each level of a coding dimension should be easily and readily distinguishable from the other levels.
Additional Information: For example, if color is used, the different colors should be easily discriminated. Each color should have a single, precise meaning that is consistent with applicable population stereotypes. A formal coding scheme that encompasses all coding methods (e.g., color, shape, brightness, textures/pattern, and flash rates) and specifies a hierarchical order should be established and formally documented. Alarms should be organized into categories according to priority. Coding should be systematically applied such that alarm information with the highest priority is also most prominent.[6105]

4.2.6.1-3 Single Coding Dimensions

Each technique used to code alarms should represent only one dimension of the alarm classification.
Additional Information: If flash rate is being used to indicate alarm state (e.g., unacknowledged, acknowledged, or cleared), it should not also be used to indicate need for user action (e.g., immediate action required, action required within 15 minutes, or no near- term action needed).[6105]

4.2.6.1-4 Coding Complexity

The number of different coding techniques should be kept to a minimum, so that the coding system does not become too difficult to use or understand.[6105]

4.2.6.2-1 Visual Coding for Importance

A visual coding method should be used to indicate alarm importance and should be consistently applied throughout the alarm system.
Additional Information: To be effective, an alarm system should attract attention and help the operator focus attention on more-important rather than less-important alarms. A flashing visual signal is a preferred means for directing attention and indicating alarm status (e.g., unacknowledged, acknowledged, and cleared-not reset) on SDCV and computer-based displays.[6105]

4.2.6.2-2 Redundant Priority Coding

Redundant codes (e.g., color and location) should be used for alarms that require rapid action.[6105]

4.2.6.2-3 Flash Rate

Flash rates should be from three to five flashes per second with approximately equal on and off times.[0700]

4.2.6.2-4 Brightness Levels for Transilluminated Displays

For transilluminated displays, such as lighted alarm tiles, the luminance of the dim state (if used) should be at least 10 percent greater than the inactivated state; the brightest state should not be more than 300 percent of the surrounding luminance.
Additional Information: Transilluminated displays should have no more than 3 levels. Brightness of 'on' alarms should not be annoying or distracting.[6105]

4.2.6.2-5 Brightness Levels for VDU Displays

For VDU displays, the bright state should be at least 100 percent brighter than the normal state.
Additional Information: VDU displays should be limited to only two levels.[6105]

4.2.6.2-6 Color Detectability

Low-intensity indications (e.g., dark red) in the periphery of the visual field should be avoided where color coding is used, since they may not be readily detected.
Additional Information: If the display system has an area that is a specific focus of attention, then displays located in adjacent areas may be frequently in the periphery of the operator's field of vision.[6105]

4.2.6.2-7 Spatial Coding

Spatial coding may be used to indicate alarm importance.
Additional Information: Spatial coding is related to alarm organization, which is addressed in Section 4.5.7.[6105, 6684]

4.2.6.2-8 Suppressed Visual Codes

If the visual codes indicating alarm status are automatically suppressed or delayed during high alarm volume conditions or the presence of more important alarms, they should be automatically presented after the more important alarms have been addressed.
Additional Information: Under high alarm volume conditions, the designer may consider suppressing or delaying the alerting indications (e.g., visual flashing) for those alarm conditions that (1) do not require immediate response, and (2) do not indicate a challenge to plant safety and technical specifications. This will assist operators in detecting the more significant alarm messages and reduce distraction from less important ones. Plant personnel should not be required to remember to request alarms that have been automatically suppressed.[6105]

4.2.6.3-1 Audio Signals for Alarms

An auditory signal should be used to alert the user to the existence of a new alarm, or any other condition of which the user must be made immediately aware.

Additional Information: Auditory cues should be provided for all new alarms under normal operating conditions. However, under off-normal conditions where high alarm density exists, the designer should consider suppressing the auditory signal for those alarmed conditions that (1) do not require immediate response and (2) do not indicate a challenge to plant safety and technical specifications. For example, audio signals associated with clearing alarms might be omitted under certain circumstances. This will prevent operators from being distracted by less important alarms while attending to more significant ones. Some designs may have a timed audible signal rather than one that is continuous until acknowledged. In this case, see the guideline for reminder audible signals, below.[6105]

4.2.6.3-2 Auditory Coding of Remote Alarms

Auditory coding techniques should be used when the workstation associated with the alarm is not in the main operating area.

Additional Information: During off-normal conditions, the designer should consider the suppression of the auditory code for those alarms that (1) do not require immediate response and (2) do not indicate a challenge to plant safety and technical specifications. This will prevent operators from being distracted by less important alarms while attending to more significant ones.[0700]

4.2.6.3-3 Distinguishable Auditory Signals

The auditory signal associated with a SDCV alarm should be easily distinguishable from the auditory signal associated with an alarm message displayed by other means (e.g., on a VDU message display).[6105]

4.2.6.3-4 Audible Signals for Alarm States

The tones used for incoming alarms should be separate and distinct from tones used to signify "clearing" alarms.[6105]

4.2.6.3-5 Reminder Audible Signals

If the tone associated with an unacknowledged alarm automatically turns off after an interval of time, a reminder tone should be presented to alert the user to the continued presence of an unacknowledged alarm.

Additional Information: The same principle holds for alarms that may have had the auditory code suppressed because of high alarm conditions or the presence of more important alarms. When the more important alarms have been addressed, the alarm system should remind the operator, via visual or auditory signals, of the presence of the unacknowledged alarms.[6105]

4.2.6.3-6 Reset of Auditory Alert

The auditory alert mechanism should automatically reset when it has been silenced.[0700]

4.2.6.3-7 Interference Among Signals

Audio alarm signals should not conflict with other auditory codes or signals.

Additional Information: If continuous, relatively loud signals are used, they may render other codes and signals less audible. Thus, it may be necessary to consider the audibility of a signal not just in the presence of ambient control room noise, but also in combination with other signals that might plausibly occur at the same time. To avoid mutual masking, the frequencies of tonal signals associated with alarms that may be active at the same time should be separated by at least 20 percent of the center frequency. Interference among alarm signals is less of a concern if the signals consist of a number of widely separated frequency components or of brief groups of pulses presented at intervals. Techniques are available that allow the audibility of signals in noise to be predicted.[6105, 6684, 0700]

4.2.6.3-8 Readily Identifiable Source

The user should be able to quickly determine where to direct attention (e.g., which functional area of the plant or which station) from the characteristics of the auditory alert and/or the source from which the auditory alert originated.

Additional Information: This guideline pertains to the use of auditory tones to direct the operator to the location of a spatially fixed alarm display device in order to expedite the operator's response to the alarm condition. The use of sound to indicate the location of the alarm display may be of less value if the advanced alarm system allows the same alarm message to be retrieved from multiple locations (e.g., from redundant VDUs) in the control room. It should also be noted that in advanced control rooms that feature compact control consoles, the alarm display devices may not be physically separated enough to use sound localization as a cue. In this case, coded audio signals (possibly from a single source) would be used to direct the operators' attention. Thus, this guideline is most appropriate for advanced alarm systems that feature spatially fixed alarm display devices. It has been recommended that coded signals from a single audio source should not be used to identify individual workstations within the main operating area, and that each major console should be equipped with a separate sound generator capable of producing a distinctive sound. If the direction of a source sound is to be used as a cue, the signal should not be a high-frequency pure tone, since such signals can be difficult to localize.[6105, 6684, 0700]

4.2.6.3-9 Signal Level

The signal intensity should be such that users can reliably discern the signal above the ambient control room noise.

Additional Information: The intensity of an audio signal should be such that users are alerted aurally to an alarm occurrence under the most adverse anticipated background noise conditions. A signal level 10 dB(A) above average ambient noise is generally considered adequate. It has also been recommended that sound intensity should be limited to a maximum of 95 dB(A), but that signal levels of 115 dB(A) may be used if considered absolutely necessary to achieve required attention-getting reliability for alarms indicating extreme danger. The tendency for designers to err on the side of conservatism results in many audio signals being more intense than is necessary to ensure reliable detection (see Guideline 4.2.6.3-10, Design of Audio Signals).[6105, 0700]

4.2.6.3-10 Design of Audio Signals

Audio signals should be designed to minimize irritation and startle.

Additional Information: Signals should reliably capture the user's attention but should not be unpleasant. Considerations include the selection of signal frequency and intensity, and the overall design of the audible alarm scheme.[6105, 0700]

4.2.6.3-11 Manual Disable/Adjustment of Signal Intensity

Manual disable or adjustment of auditory signal intensity (loudness) should be avoided.

Additional Information: The need to adjust auditory signal level can be alleviated by improved signal design and level selection. If signal level is adjustable, it should be controlled by administrative procedure. Under no circumstances should users be able to disable audio alarm signals or reduce their level so as to render them inaudible.[6105, 0700]

4.2.6.3-12 Sound Sources

The number and placement of loudspeakers should be such that auditory signals are free of distortion and are equally audible at any workstation in the control room.

Additional Information: Speakers should be oriented away from surfaces that could scatter or diffuse the acoustic wave. Speakers should not be located behind structures that could cause distortion, echoes, or sound shadows. When sound localization is used to direct the operator to particular alarm display devices, the loudspeakers should be oriented such that their location can be quickly discerned and corresponds to the location of the intended alarm display device. Loudspeakers for adjacent alarm display devices should have adequate separation to allow their individual locations to be discerned.[6105, 0700]

4.2.6.3-13 Auditory Signal Discriminability

Each audio signal should be unambiguous and easily distinguishable from every other tone in the control room.

Additional Information: Current sound generation technology allows the design of alarm signals that make better use of the operator's ability to process audio information. It is possible to design signals that are not only more discriminable from one another than are conventional signals, but also have the potential to carry more information. Signals should be composed of unique combinations of tone pattern and frequency. See also Guideline 4.2.6.3-8.[6105, 6684, 0700]

4.2.6.3-14 Number of Tonal Signals

When information is coded by the pitch of narrow-band signals (i.e., tones), no more than three frequencies should be used.

Additional Information: The frequencies should not be in a ratio of 2:1 with one another, since it can be difficult to identify pitches an octave apart. Although some sources recommend that no more than five separate frequencies should be used, operators may not reliably distinguish among more than three pitch codes. For critical alarms with differing response requirements, the more conservative guidance should be followed. If more than three critical alarms are to be coded, it is preferable to combine pitch with another dimension to create more distinctive signals. See Guideline 4.2.6.3-13.[6105]

4.2.6.3-15 Frequency of Tonal Signals

Center frequencies should be widely spaced within a range of from 500 to 3,000 Hz, although a wider range of from 200 to 5,000 Hz may be acceptable.

Additional Information: It is recommended that tonal signals be broad band and widely spaced within the 200 to 5000 Hz range.[6105]

4.2.6.3-16 Pulse Codes

No more than three pulse repetition rates should be used for coding purposes.

Additional Information: Repetition rates should be between 1 and 8 pulses per second, since faster rates may not be perceived as pulses. Repetition rates should be sufficiently separated (e.g., differ by a factor of 2) to ensure operator discrimination. Sounds with the same temporal pattern, including signals with similar duty cycles (on-off times), may be confused, despite having very different pulse speeds (i.e., periods). Such signals are therefore more appropriate for coding the level of urgency of a condition than for indicating different types of conditions.[6105, 6684, 0700]

4.2.6.3-17 Number of Frequency Modulated Signals
No more than three modulated frequency codes for audible alarms should be used.
Additional Information: Warbling sounds, with frequencies modulating from 1 to 3 times per second, are attention-getting as well as easily recognized, whereas slower modulation rates do not develop distinguishable characteristics rapidly enough to be appropriate for alerting applications.[6105]

4.2.6.3-18 Center Frequency of Frequency Modulated Signals
If modulation of frequency (Hz) of a signal is used to denote information, the center frequencies should be between 500 and 1000 Hz.[0700]

4.2.6.3-19 Audio Pattern Codes
If sequences of tones are used to represent information, the patterns should be easily recognizable.
Additional Information: Warning sounds consisting of "bursts" composed of five or more brief pulses (about 0.1 second in duration) with inter-pulse intervals of .15 to .3 seconds have been recommended. The pulses may be designed to be distinctive with respect to their onset and offset shaping, fundamental frequency, and harmonic structure. The bursts may vary as to the number of pulses, the tempo at which they are presented, and the rhythmic and pitch contours.[6105]

4.2.6.3-20 Compound Codes
A maximum of nine auditory signals should be used when coded in two or more dimensions.
Additional Information: When signals differ in two or more dimensions (e.g., pitch and temporal pattern), a greater number of signals can be reliably distinguished. This maximum includes auditory signals used outside of the control room (e.g., fire alarm or site emergency alarm).[6105, 6684]

4.2.6.3-21 Intensity Coding
Coding of auditory signals by intensity (loudness) should not be used.
Additional Information: The range of intensities between the level required to ensure audibility and the level at which signals become aversive can be relatively narrow; the usefulness of this dimension for coding is therefore limited. If such coding must be used, no more than two levels should be defined. The signals should differ from each other by a minimum of 6 dB(A). The lower intensity should be about 10 dB(A) above the ambient noise level, and the maximum signal-to-noise ratio should be 10 dB(A) for most applications of sound intensity coding. It is recommended that sound intensity should be limited to a maximum of 95 dB(A), but that signal levels of 115 dB(A) may be used if considered absolutely necessary to achieve required attention-getting reliability for alarms indicating extreme danger. Whether this coding would be effective would depend on the frequency spectrum of the ambient control room noise and the frequency of the signal.[6105, 0700]

4.2.6.3-22 Speech Presentation of Alarm Information
Using speech alone for presenting alarm information is not recommended.
Additional Information: Speech is an acceptable medium for presenting interface-related information (see Section 1.2.12, Speech Displays), and there may be advantages associated with using speech for presenting alarm information as well. However, its appropriateness has been questioned for tasks where there is a memory component, there is likely to be some delay before the fault is attended to, there is likely to be more than one alarm presented at a time, and the operator is required to assimilate information from a variety of sources using spatial reference. Therefore, it has not yet been shown that it is an appropriate method for presenting alarm information in process control contexts. Speech should only be used in conjunction with other methods of presenting alarm information.[6684]

4.2.7.1-1 Functional Grouping of Alarms

Alarms within a display should be grouped by function, system, or other logical organization.
Additional Information: Alarm elements should be grouped so that system functional relationships are readily apparent. For example, area radiation alarms should be grouped on one display, not spread throughout the control room. As much as possible, the alarms should be grouped with controls and displays of the same system.[6105, 6684, 0700]

4.2.7.1-2 Visual Distinctness of Functional Groups

Alarm functional groups should be visually distinct from one another.
Additional Information: Although the concept of functional grouping is typically applied in the context of spatially dedicated, continuously visible displays, it can be applied to alarm lists as well. Segregating alarm messages by plant system may allow operators to direct their attention more effectively, especially when individual members of a crew are assigned principal responsibility for different plant systems.[6105, 6684]

4.2.7.1-3 Group Labels

System/functional groups should be clearly delineated and labeled such that the operating crew can easily determine which systems have alarms that have not yet cleared and which system is affected by a particular incoming alarm.[6105]

4.2.7.1-4 Coordinate Designation Identifiers

If alarm displays are organized in matrices, the vertical and horizontal axes of the displays should be labeled with alphanumerics for ready coordinate designation of a particular visual element.[0700]

4.2.7.1-5 Density of Alarm Elements

An alarm tile display matrix should contain a maximum of 50 alarms.
Additional Information: Matrices smaller than 50 alarms are preferred.[0700]

4.2.7.1-6 Logical Arrangement of Alarms

Alarms should be ordered to depict naturally occurring relationships.
Additional Information: Naturally occurring relationships (e.g., those derived from the physical process) include the following:

- pressure, flow, level, and temperature alarms in fluid systems;
- alarms for a given thermodynamic parameter at different points within the system that indicate a progression (e.g., within a fluid system, a series of pressure alarms starting with the source tank and ending with the system discharge);
- several alarms for the same variable indicating levels of severity (e.g., tank level low and tank level low-low); and
- alarms related by cause and effect.

For example, pressure, flow, level, and temperature could be arranged left-to-right.[6105]

4.2.7.1-7 Consistent Ordering

Alarm parameters (e.g., pressure, flow, level, and temperature) arranged in one order on one panel should be arranged in the same order on other panels.

Additional Information: Circumstances may dictate different orderings for systems with very different functions. However, once an arrangement has been chosen, the arrangement should be used consistently within similar systems or alarm groups.[6105]

4.2.7.1-8 Alarm Display Identification Label

Each group of alarm displays should be identified by a label above the display.

Additional Information: A group of displays could be a panel of tiles or a group of tile-format VDU displays.[0700, 6105]

4.2.7.2-1 Listing by Priority

Lists of alarm messages should be segregated by alarm priority with highest priority alarms being listed first.[6105]

4.2.7.2-2 Message Listing Options

In addition to priority grouping, users should have the capability to group alarm messages according to operationally relevant categories, such as function, chronological order, and status (unacknowledged, acknowledged/active, cleared).

Additional Information: For example, it should be possible to list alarm messages in chronological order with the most recent messages placed at the top of the stack (i.e., alarm messages entered in a pushdown stack mode). Grouping alternatives should not interfere with the detection of high-priority alarms. The grouping should be easy to implement.[6105, 6684]

4.2.7.2-3 Blank Lines

Alphanumeric alarm lists should have a separation (blank row) between every four or five alphanumeric messages.[6105]

4.2.7.2-4 Scrolling of Message List

The method of adding alarm messages to the list should preclude message scrolling.

Additional Information: Scrolling makes it difficult to read alarm messages, especially when many alarms are coming in. An alternative method of viewing alarm lists, such as paging, is preferred.[6105]

4.2.7.2-5 Message Overflow

Alphanumeric alarm messages that overflow the first page of alarm messages should be kept on subsequent alarm pages.

Additional Information: Important alarm information should not be truncated solely because the immediate display space is exceeded. In addition, the alarm system should clearly indicate that additional information is available in subsequent pages.[6105]

4.3.1-1 Access to Undisplayed Unacknowledged Alarms

A VDU-based alarm system should provide rapid access to any unacknowledged alarm messages that are not shown on the current display.

Additional Information: When an alarm has been indicated, e.g., by an auditory signal, plant personnel should have rapid access to the alarm information that describes the nature of the alarm condition.[6105]

4.3.2-1 Global Silence Capability

It should be possible to silence an auditory alert signal from any set of alarm system controls in the main operating area.

Additional Information: A global silence capability together with separate silence and acknowledge capabilities can be useful during high alarm situations. It can allow the operator to silence many distracting alarms and then acknowledge these alarms at their respective panels. It is not necessary that silence capability be provided only where the specific alarm can be read, so long as the operator is made aware of all alarms that are being silenced. That is, the operator should not be able to silence alarms that cannot be visually detected from the global silence control. The primary purpose of the auditory signal is to alert the operator to a new alarm. Once alerted, the operator refers to visual indications of the specific alarm and its message. The auditory signal can rapidly become distracting and irritating to the operators. It should be possible to silence an audible cue from either a VDU or a tile panel control station (see also Guideline 4.3.5-3).[0700, 6105]

4.3.2-2 Manual Silencing

Auditory signals should be silenced manually unless this interferes with other more critical actions.

Additional Information: While manual silence is a generally desirable feature to get the operator's attention, it may become distracting to manually silence all alarms under high-alarm conditions. Guidelines 4.3.5-3 and 4.3.6-3 address alarm system configuration changes made either automatically or by operator-selection, such as automatic silence of auditory alerts for lower priority alarms under high-alarm conditions.[6105]

4.3.3-1 Effect of Acknowledge Function

An alarm acknowledgment function should cause the alarm's visual coding to change from that indicating an unacknowledged alarm to a visually distinct ' not cleared' state.
Additional Information: For example, the acknowledge function might cause an alarm to change from flashing to steady. (See also Guideline 4.2.3-4.)[0700]

4.3.3-2 Acknowledgment Locations

Acknowledgment should be possible only from locations where the alarm message can be read.
Additional Information: If alarm information is available at multiple VDUs, then operators should be capable of acknowledging the alarm from the VDU at which they are working. If alarm information is presented on a large control room overview display, operators should be able to acknowledge it from alarm control locations where it can be seen. This flexibility will minimize disruption caused by the alarm system interactions. It should not be possible to acknowledge alarms from locations where they cannot be read. If alarms can be acknowledged from multiple locations, then a means should be provided for ensuring that all operators for whom the alarm is important are aware that the alarm occurred. These means may include spoken, telephone, or computer-based communications between personnel.[6105]

4.3.3-3 Acknowledgment of Alarm Messages

Non-SDCV alarms should only be acknowledged when the alarm message is on the screen.
Additional Information: Alternatively, the acknowledgment action may display the alarm message.[6105]

4.3.4-1 Effect of Reset Function

The reset function should place an alarm in an unalarmed state after the condition has cleared.
Additional Information: The reset function should silence any audible signal indicating clearance and should extinguish the light and return the alarm to an inactive state. Note that some alarms may have automatic reset, when it is not necessary that the operators specifically know the reset condition.[0700]

4.3.4-2 Appropriate Use of Manual Reset

A manual reset sequence should be used where it is important to explicitly inform users of a cleared condition that had once been deviant.
Additional Information: An automatic reset sequence should not be used in this situation.[6105]

4.3.4-3 Appropriate Use of Automatic Reset

An automatic reset sequence should be available where users have to respond to numerous alarms or where it is essential to quickly reset the system.
Additional Information: A manual reset sequence should not be used in high-workload situations in which the time and attention required to reset the alarms may detract from other, more-critical tasks.[6105]

4.3.4-4 Reset Function Location

The reset function should be effective only from locations at which plant personnel know which alarm they are resetting.[0700, 6105]

4.3.5-1 User-Selectable Alarm System Configuration

If the alarm system provides user-selectable operational configurations, then these configuration changes should be coupled with an indication of the present configuration.

Additional Information: Alarm systems allow users to select alternative functional configurations of the alarm system under some alarm situations, such as automatic silence of auditory alerts for lower priority alarms under high-alarm conditions. Another example may be operator selection of an alarm message suppression mode in which low priority messages are not presented via the alarm displays but may be accessed through operator action. It is important that the alarm system informs the operators that a requested change in system configuration has been successfully achieved. In addition, a prominent display of the present configuration should be available.[6105, 6684]

4.3.5-2 Acknowledgment of Alarm System Configuration Changes

Acknowledgment (or confirmation) should be required if a significant alarm system configuration change is to be made by user selection.

Additional Information: Alarm systems allow users to select alternative functional configurations of the alarm system under some alarm situations. An example may be operator selection of an alarm message suppression mode in which low priority messages are not presented via the alarm displays but may be accessed through operator action. It is important that the alarm system informs the operators that a requested change in system configuration has been successfully achieved. In addition, a prominent display of the present configuration should be available.[6105]

4.3.5-3 User-Defined Alarms/Setpoints

The alarm system may provide temporary, user-defined alarms and user-defined set points for specific conditions where such alarms are determined to be of assistance in selected evolutions (e.g., temporary alarms to support increased monitoring of a problem component, or at other times when the user wants to know of a parameter trend that is approaching a limit).[6105]

4.3.5-4 Interference of User-Defined Alarms/Setpoints with Existing Alarms

User-defined alarms and setpoints should not override or interfere with the existing alarms and setpoints.[6105]

4.3.5-5 Indication of User-Defined Alarms/Setpoints

The alarm system should provide clear indication of user-defined alarms and setpoints as distinct from the alarm/setpoints designed into the system.[6105]

4.3.5-6 Control of User-Defined Alarms/Setpoints

The definition and removal of operator-defined system characteristics should be under administrative controls.[6105]

4.3.6-1 Automated Alarm System Configuration

If the alarm system automatically changes operational configurations under some alarm situations, then these configuration changes should be coupled with an alert to the user and an indication that the configuration has changed.

Additional Information: Alarm systems may provide automated functions under some alarm situations, such as automatic silence of auditory alerts for lower priority alarms under high-alarm conditions. It is important that operators be notified of the change in system functioning. In addition, a prominent display of the present configuration should be available to remind operators of the current configuration of the system.[6105]

4.3.6-2 Acknowledgment of Automatic Alarm System Configuration Changes

Acknowledgment (or confirmation) should be required if a significant alarm system configuration change is to be made automatically.

Additional Information: Alarm systems may allow users to select alternative functional configurations of the alarm system under some alarm situations, such as automatic silence of auditory alerts for lower priority alarms under high-alarm conditions. It is important that the alarm system informs the users that a requested change in system configuration has been successfully achieved. In addition, a prominent display of the present configuration should be available.[6105]

4.3.6-3 Automatic Mode-Defined Setpoints

The need for operator acknowledgment of system-generated setpoint changes based on plant mode should be evaluated on a case-by-case basis.

Additional Information: Alarm systems may alter setpoints in an effort to minimize nuisance alarms. While such changes may be associated with well-understood, easily recognizable plant conditions, others may be less familiar and not readily understood by plant personnel. In the latter situation, plant personnel may misunderstand the alarm information because they do not realize the setpoints have changed. When this situation is of concern, confirmation of the change should be considered.[6105]

4.3.7-1 Separate Controls for Alarm Functions

Separate controls should be provided for silence, acknowledgment, reset (acknowledging an alarm that has cleared and returning it to normal), and testing.

Additional Information: A global silence capability together with separate silence and acknowledge capabilities can be useful during high alarm situations by allowing the user to silence many distracting alarms and then acknowledge these alarms at their respective panels. A variety of controls is possible, such as pushbuttons, function keys, and on-screen controls.[6105, 0700]

4.3.7-2 Distinct Coding of Control Functions

Alarm system controls should be distinctively coded for easy recognition.

Additional Information: The controls should be distinguishable from each other, by touch and sight, to prevent accidental operation of the wrong control. Such techniques as color coding, color shading the group of alarm controls, demarcating the group of alarm controls, or shape coding should be used.[6105, 0700]

4.3.7-3 Consistent Layout of Control Group

Each set of alarm system controls should have the functions in the same relative locations.

Additional Information: Consistent locations should be established for silence, acknowledge, reset, and test operating sequence controls.[6105, 0700]

4.3.7-4 Separate Controls for Tile and VDU Alarms

If the alarm system contains both alarm tiles and VDU alarm displays, each should have its own set of controls.

Additional Information: If alarm information is presented redundantly on tile and VDU displays, then alarm acknowledgment via one device (i.e., either the VDU or tile panel control station) should cause the redundant alarm to be automatically acknowledged on the other device. All other control actions (acknowledge, reset and test) should be specific to the workstation associated with the alarm (see also Guideline 4.3.2-1).[6105]

4.3.7-5 Defeating Controls

Alarm system control designs should not allow the controls to be altered or defeated.

Additional Information: For example, some pushbuttons used for alarm silencing and acknowledgement can be held down by inserting an object in the ring around the pushbutton. While the controls should be designed to prevent their being defeated, the system should be designed to minimize the desire to do so.[6105, 0700]

4.4.1-1 Design for Reliability

The alarm system should be designed so that no single failure will result in the loss of a large number of alarms.

Additional Information: Also, the failure of a single alarm system component should not result in the loss of an individual alarm important to plant safety.[6105]

4.4.1-2 VDU Reliability

Where alarms are presented on a VDU as the primary display, users should be able to access the alarms from more than one VDU.

Additional Information: Failure of a single VDU should not prevent access to VDU-based alarm presentations at the main workstation. Alarm printer displays should not be the only back-up to a VDU display.[6105]

4.4.1-3 Dual Light Bulbs

Annunciator tile-type displays should be designed with dual light bulbs so that a single bulb failure will not interfere with detection of the alarm condition.

Additional Information: Alarm system displays should be designed with a high level of reliability. In the case of annunciator tile displays, each tile should be illuminated by two or more lights to protect against loss of indication due to failure of one.[6105]

4.4.1-4 Flasher Failure Mode

In case of flasher failure, an unacknowledged alarm should assume a highly conspicuous state such as a steady on (e.g., illuminated) state rather than a less conspicuous state such as off.

Additional Information: While it is preferable in the case of a flasher failure for the associated alarm element to remain on (e.g., illuminated) rather than off, a unique and highly conspicuous code is best. The code should be unique to prevent confusion between unacknowledged and acknowledged alarms. It should be salient to alert the operator to the malfunction of the alarm display system. In addition, other alerting mechanisms such as warning messages may be used to inform the operator of a malfunction in the alarm display system.[0700, 6105]

4.4.2-1 Testing Capabilities

Test controls should be available to initiate operability tests for all essential aspects of the alarm system (including processing logic, audible alarms, and visual alarm indications).
Additional Information: For those portions of the alarm system (such as audible alarms and visual indications), the test capability should be simple and available to the operators. The more complex portions (such as sensor inputs and logic processing) should also be testable, but by I&C technicians and engineers. Advanced alarm systems, having capability for continuous, on-line, self-testing may satisfy some of these recommendations.[0700, 6105]

4.4.2-2 Testing Requirement

Periodic testing of the alarm system should be required and controlled by administrative procedure.
Additional Information: Simple functional tests are normally required once per operating shift. Reliability analyses of the alarm system may be used to determine appropriate intervals and degree of testing to be performed on the alarm system.[0700]

4.4.3-1 Design for Maintainability

The alarm system should be designed so that maintenance activities can be performed with minimal interference with the activities of the users.

Additional Information: Desirable design features may include built-in test capabilities, modular components that can be rapidly removed and replaced, and rear access panels which prevent maintenance activities for obstructing the users' view of controls and displays.[6105]

4.4.3-2 Tagged-Out Alarms

Tagging out an alarm (taking it out of service) should require disabling of the associated visual and audio signals.

Additional Information: A tagged-out alarm should never be lit or flashing, and should never cause any audible device to sound.[6105]

4.4.3-3 Out-of-Service Alarm Indication

Cues for prompt recognition of an out-of-service alarm should be designed into the system.

Additional Information: Tagging out an alarm should not prevent its identification and should not obscure any other alarm or interfere with operations.[6105, 0700]

4.4.3-4 Extended Duration Illumination

If an alarm tile must be 'on' for an extended period during normal operations because of equipment repair or replacement, it should be (1) distinctively coded for positive recognition during this period, and (2) controlled by administrative procedures.[0700]

4.4.3-5 Tile Cover Replacement

If a lamp replacement requires legend tile removal, there should be a way to ensure that the tile is replaced in the correct location.

Additional Information: The alarm element and/or the replacement task should be designed to prevent incorrect positioning of the cover, legend, or tile. For example, annunciator tiles might be permanently marked with a unique identifier specifying their position in the alarm window matrix. Alternatively, it might be administratively required that no more than one tile cover be removed from the matrix at a time.[6105, 0700]

4.4.3-6 Hazard Avoidance

Lamp replacement should not pose an electrical shock hazard.[0700]

4.4.3-7 Aids for Alarm System Maintenance

Aids should be provided, if needed, to assist personnel in performing alarm system maintenance.

Additional Information: Aids include instructions and specialized tools. For example, aids may be needed to support changing of light bulbs in the alarm system.[0700]

4.4.4-1 Alarm System Failure Indication

Users should be given prompt indication of a failure of the alarm system or its major subcomponents.[6105]

4.5-1 ARP Scope

ARPs should be available for alarm conditions that require a response that affects the plant process control system or plant equipment.

Additional Information: Minor alarms associated with data input errors or computer space navigation errors may not require ARPs. In addition, other alarms such as those in alarm systems that are separate from the main process alarm systems and require simple responses, may not need ARPs. In this latter case, the lack of ARPs should be specifically considered and justified.[5908]

4.5-2 ARP Access

Users should have immediate access to ARPs from the location at which the alarm messages are read.

Additional Information: An operator should not be required to leave the location at which the alarm message is displayed in order to access ARP information. In a tile system, the identification and indexing of ARPs should be consistent with the method of identifying the alarm. The means used for identifying row and column locations of alarms should be distinct so that possible confusion of these identifiers is avoided. A computerized system may display the appropriate procedure for a given alarm on a VDU when the operator "selects" the alarm message.[6105, 6684]

4.5-3 ARP Content

ARPs should contain the following information:

- The system/functional group to which the alarm belongs,
- The exact alarm text or legend,
- The alarm source (i.e., the sensor(s) sending the signal, processors and signal validation logic, and the actuating device(s) for the alarm with a reference to a schematic diagram on which such devices can be found),
- Alarm setpoints,
- Priority,
- Potential underlying causes for the alarm (e.g., low water level - inadequate feed flow),
- Required immediate actions, including actions that can be taken to confirm the existence of the alarm condition,
- Actions which occur automatically when the alarm occurs (and which should be verified as having taken place),
- Followup actions,
- Explanations of relevant alarm processing (e.g., comparisons and combinations of plant parameters; alarm filtering and suppression; alarm setpoints that are conditional, such as setpoint values and time delays used to prevent the occurrence of nuisance alarms when a parameter oscillates in an out of the alarm range), and
- Pertinent references.

Additional Information: Users should be given information (such as that associated with 'alarm source' in the guideline) that they can use to confirm the existence of alarmed conditions.[6105, 6684]

4.5-4 Information Consistency with the HSI

Information contained in the ARPs should be consistent with information on control boards, in the alarm system, in I&C procedures used to calibrate alarm setpoints, in controlling documents that determine setpoints (e.g., Technical Specifications and accident analyses), in P&IDs, in emergency operating procedures, and in other plant procedures.[6105]

4.5-5 Presentation Consistency with the HSI

The terminology, conventions, standards, and codes used in the presentation of the ARPs should be consistent with the rest of the HSI.

Additional Information: The ARPs should use the same conventions, such as terminology for plant systems and equipments, identification codes for plant components and parameters, and measurement units, that are used in the main HSI displays and procedures. Defined values, such as alarm setpoints, should be consistent. In addition, information coding schemes used in the ARPs should be consistent with the rest of the HSI. For example, if graphical displays are used in the presentation of the ARPs , then coding conventions, such as symbols, icons and color, should be consistent with the rest of the HSI, such as information presented via plant displays and computer-based systems for emergency operating procedures. For example, if color codes are used to indicate priority, it should have the same meaning across all displays of the HSI.[6684]

4.5-6 ARP Format

The ARP format should:

- Highlight the ARP identifier on each page of the procedure,
- Highlight important items,
- Locate information categories in the same position on each page,
- Consistently present information throughout the ARP, and
- Minimize the need for paging back and forth to obtain the information.[6105]

4.6-1 Display and Line of Sight
Visible alarm indications should be located within about 60 degrees on either side of the direct line of sight of the user's normal work position.[6105]

4.6-2 Location of Alarm System Displays and Controls
Alarm displays and controls should be located so that the display can be read while operating the controls.[6105]

4.6-3 Location of First-Out Alarms
First-out displays should be located at the main workstation for the system and/or at a plant overview display visible to the crew.[0700]

4.6-4 Consistent Ordering
The ordering (e.g., left-to-right positioning) of displayed alarm groups should be consistent with the ordering of displays and controls of related plant systems and components.[6105]

4.6-5 Location for Prompt Response
Alarm displays and controls should be arranged and located such that those in the control room who must respond to an alarm can access the alarm information in sufficient time to respond adequately.[6105]

4.6-6 Location for Access to Process Controls and Displays
Visual alarm panels should be located near the controls and displays which are required for corrective or diagnostic action in response to the alarm.
Additional Information: If displays and controls associated with an alarm are on different panel segments, ensure that the alarm displays are located near the process display segment. If they are presented on a VDU, easy access to supporting controls and displays should be provided in the display.[6105, 6684, 0700]

4.6-7 Interference from Nearby Lights
Indicator lights or other non-alarm illuminated displays should not be located so close to alarm displays that they could be mistaken for an alarm or mask an alarm.[6105]

4.7-1 Consistency with the Main HSI

The alarm system HSI should be consistent with the standards and conventions used for the HSIs for other displays and controls in the control room.

Additional Information: The alarm system should use the same conventions such as symbols, icons, acronyms, coding, and measurement units that are used in the main HSI displays and procedures. While some minor differences may exist, the alarm system should never use a display feature, such as coding, in a way that is different from or conflicts with other HSIs. For example, if color is used to code priority, it should have the same meaning in the alarm system as in the process displays.[6105]

4.7-2 Consistency with Emergency Operating Procedures

The alarm system HSI should be consistent with the standards, conventions, and terminology used in the plant emergency operating procedures.

Additional Information: The alarm system should use the same conventions, such as terminology for plant systems and equipment, identification codes for plant components and parameters, and measurement units, that are used in the main HSI displays and procedures. Defined values, such as alarm setpoints, should be consistent. In addition, if the procedures use coding to present information, such as in graphical displays of a computer-based procedure system, then the alarm system should use the same conventions, such as symbols, icons and coding. For example, if color is used to code priority, it should have the same meaning in the alarm system as in the displays of a computer-based emergency operating procedure.[6684]

4.7-3 Conformance to HSI Design Review Guidelines

Alarm system elements (e.g., displays and controls) should conform to general HSI guidelines as well as alarm system guidelines.

Additional Information: While the alarm system guidelines take precedence over other more general HFE guidelines, it should be kept in mind that the alarm system is a part of the overall HSI. As such, it should conform to the same guidelines for general display and control design. For example, if the alarm system uses a touch screen interface for operator input and query of the system, the review guidelines for touchscreens (Section 3.2.4, Touch Screens, Light Pens, and Graphic Tablets) should be used to evaluate that aspect of the interface. As another example, if the alarm displays are integrated into P&ID VDU displays, the P&ID aspect to the display, such as icons and symbols, should be evaluated using Sections 1.2.8, Mimics and Diagrams, and 1.3.4, Icons and Symbols. In the event of overlap or conflict in guidelines, the guidelines for alarm systems take precedence when reviewing the alarm system.[6105]

SECTION 5: SAFETY FUNCTION AND PARAMETER MONITORING SYSTEM

5 SAFETY FUNCTION AND PARAMETER MONITORING SYSTEM

The primary function of these monitoring systems, which operate during all plant conditions, is to present information to aid control room personnel during abnormal and emergency conditions in determining the safety status of the plant and in assessing whether conditions warrant corrective actions by operators to avoid a degraded core. This function is particularly important during anticipated transients and in the initial phase of an accident.

INFORMATION DISPLAY

The devices used to display this information may include conventional and computer-based devices, as described in Section 1.6, Display Devices. Conventional display devices include meters, light indicators, numeric readout displays, plotters, and plotters. Computer-based display devices include CRTs, flat panel devices, and large-screen devices.

These devices may have single or multiple display functions. A single-function device presents information in a fixed format. Examples include an indicator that presents a single variable and a visual display unit that presents a single page containing a set of variables. A multiple-function device contains a set of display pages through which the user navigates to access desired information.

The organization of this information (e.g., grouping) of related data is important for supporting prompt recognition and comprehension of plant status. Related information may be organized by the physical arrangement of single- and multiple-function display devices. For example, individual devices may be grouped together so that related variables are presented in the same portion of a console or panel. Within a multiple-function device, the information is also organized by its placement within a display page and by the arrangement of display pages.

The information presented by these monitoring systems includes parameters and indications of functions important to plant safety. Important presentation characteristics include the conciseness of the display format, the arrangement of information according to plant modes, the range of conditions displayed, the display system's response to transient and accident conditions, the data sampling rate, the display's accuracy, the continuous presentation of information, the visibility of displayed data, limit marks for variables, and the indication of magnitudes and trends for variables. Guidelines for the review of these display characteristics are included in Section 5.1. General guidelines for the review of display devices, formats, and elements, and data quality are provided in Section 1.

USER-SYSTEM INTERACTION

User-system interaction refers to the types of operations that must be performed when users interact with a system. For safety parameter and function monitoring systems, this interaction may take many forms. System characteristics that affect user-system interaction include: user input formats; cursors; system response; features for managing displays; features for managing information; features for the prevention, detection, and correction of errors; and system security features. HFE review guidelines for these general topics are provided in Section 2. Because safety parameter and function monitoring systems are used to support operators during abnormal and emergency conditions, it is important that user-system interaction tasks are within the skill and workload capabilities of the users under these conditions. Guidelines addressing these considerations are provided in Section 5.2.

RELIABILITY, TEST, MAINTENANCE, AND FAILURE INDICATION FEATURES

This topic refers to features necessary for ensuring the continued operation of the safety parameter and function monitoring system. Reliability addresses the resistance of the system to failures. It affects the degree of trust that operators have regarding the displayed information and whether the system will

continue to operate correctly when needed. Failure indications addresses the ways in which the user is informed of the presence of potential failures or malfunctions in the system. These indications aid the user in identifying and diagnosing failures. Data validation techniques are used in plant I&C systems to assess the validity of plant data by comparing the data from different sources. Data that pass the test are said to be valid (i.e., of reliable quality), while data that fail are determined to be invalid (i.e., not reliable and possibly indicative of a system malfunction). Data that cannot be tested, such as when processors or redundant data are not available, are said to be unvalidated (i.e., of unknown quality). Analytical redundancy refers to one method for testing the validity of data. It is the intercomparison of measured variables, through the use of mathematical models based upon known physical relationships among variables. Another method of data validation is the direct comparison of values from redundant sensors. Guidelines for reliability, test, maintenance, and failure indication features are given in Section 5.3.

INTEGRATION WITH OTHER HSI ELEMENTS

This characteristic addresses the consistency and compatibility of the safety parameter and function monitoring system with the rest of the HSI. Because these systems are used in coordination with other display and control devices of the HSI to verify plant safety and support operators in determining corrective actions, the consistency and compatibility of conventions used for presenting and coding information and means of user-system interaction are important review considerations. Sections 1, 2, and 3 provide an extensive set of design review guidelines for information display, user-system interaction, and process control and input devices, respectively. In addition, the physical integration of the safety parameter and function monitoring systems with the rest of the HSI is an important review consideration to ensure that the system can be readily accessed and does not interfere with the use of other portions of the HSI. Guidelines for the physical integration of the monitoring system with the rest of the HSI are provided in Section 5.4.

5 SAFETY FUNCTION AND PARAMETER MONITORING SYSTEM

5.1 Information Display

5.1-1 Convenient and Ready Access to Data

Plant parameters and variables important to safety should be displayed in a way that is convenient and readily accessible.

Additional Information: The displays should be accessible to the following personnel, although not necessarily at the same time: shift supervisor, senior reactor operator, reactor operator, and shift technical advisor.[0800]

5.1-2 Critical Safety Function Display Visibility

Critical safety function displays should be readable from the workstations of users needing access to these displays.

Additional Information: User categories include shift supervisor, reactor operator, and shift technical advisor.[0800]

5.1-3 Critical Variables and Parameters

Critical plant variables and parameters should be displayed to help users evaluate the plant's safety status.

Additional Information: The set of critical plant variables is plant-specific and should be determined by the licensee/applicant. However, the display system, at a minimum, should provide information to plant operators about the following critical safety functions: reactivity control; reactor core cooling and heat removal from the primary system; reactor coolant system integrity; radioactivity control; and containment conditions.[0800]

5.1-4 Severe Accident Symptoms

The display system should display information about severe accident symptoms associated with the plant safety parameters and functions.[0800]

5.1-5 Concise Display of Information

Critical plant variables should be displayed in a concise format.

Additional Information: The display format should support users in comparing data from across related plant functions and assessing the safety status of the plant. A concise format might be achieved by presenting a group of critical variables on a single display or by arranging a set of displays (e.g., separate indicators) in a single location.[0800]

5.1-6 Display Response to Transient and Accident Sequences

The display's respond to transient and accident sequences should keep the user informed of the current plant status.[0800]

5.1-7 Rapid and Reliable Recognition of Safety Status Change

Critical safety function displays should allow users to comprehend a change in safety status in a matter of seconds.

Additional Information: These displays should incorporate accepted HFE principles to ensure user performance. For example, display formats containing patterns or visual coding that depict relationships between variables may support rapid comprehension. Patterns may be used that noticeably distort when an unsafe conditions is approached.[0800]

5.1-8 Data Sampling Rate

The sampling rate for each critical plant variable should be consistent with the users' needs for performing tasks.

Additional Information: There should be no meaningful loss of information in the presented data. The time delay from when the sensor signal is sampled to when it is displayed should be consistent with other displays of the HSI.[0800]

5.1-9 Display Accuracy

Each critical variable should be displayed with sufficient accuracy for the user to discriminate between normal conditions and those affecting plant safety status.[0800]

5.1-10 Magnitudes and Trends of Critical Variables

The display should provide magnitudes and trends for critical plant variables or derived variables.
Additional Information: Trends should be displayed with sufficient resolution in time and magnitude to ensure that rapidly changing variables can be observed and accurately interpreted. The time history should cover enough time and be accurate enough to depict the onset and development of conditions that vary from preceding normal operating conditions.[0800]

5.1-11 Continuous Display

Displays for monitoring safety parameters and functions should continuously display this information.
Additional Information: The display system maybe considered continuous even though all critical variables cannot be seen at one time. An example is a hierarchical network of displays from which the user can access specific displays for assessing the safety status of the plant.[0800]

5.1-12 Separate Display Pages for Plant Modes

Where plant operating modes impose different demands, separate display pages should be provided for each mode.
Additional Information: Some typical modes of plant operation are power operation, startup, hot standby, and hot shutdown. For each mode, the displays should contain at least the minimum set of data needed to assess the safety status of the plant. One means for accommodating the plant modes is to have a top-level display that is independent of plant mode and a set of mode-dependent subordinate display pages.[0800]

5.2-1 Critical Parameter Monitoring Support

The system should assist the user in monitoring critical parameters, especially parameters that change very rapidly or very slowly, by alerting the user when values are out of range.

Additional Information: The user may not be able to maintain attention on the slow-changing indication due to competing task demands and, thus, may not be aware that the parameter is out of range. For rapidly changing parameters, the unacceptable range might be reached before the user is able to begin monitoring the parameter. Setpoints used to indicate a change in status should be chosen to provide users with sufficient time to respond appropriately.[5908]

5.2-2 Alerts for Abnormal Conditions

Where feasible, the system should provide perceptual (audible or visual) cues to alert personnel to abnormal operation conditions that potentially warrant corrective action.[0800]

5.2-3 Alert to Higher Level Displays

While viewing secondary (lower-level) displays, a perceptual (audible or visual) cue should be provided by the safety parameter or function monitoring system to alert the user to return to the primary (higher-level) display format if significant information in that display requires user attention.[0800]

5.2-4 Ease of Interaction

User interactions with the display system should be within the skill capability of the control room crew and should not significantly increase personnel workload.

Additional Information: No additional operating staff beyond the normal control room operating crew, should be needed to operate the display during normal and abnormal plant operation. Interactions with the display system should not impose workload demands that detract from other tasks performed by control room personnel during normal and abnormal plant operations.[0800]

5.3-1 Display Reliability

The display should not give false indications of plant status.
Additional Information: Both the processing of display information and the display device should be highly reliable. The operating and failed states should be indicated to users as described in Guideline 1.1-23.[0800]

5.3-2 Data Reliability/Validation for Critical Plant Variables

Critical plant variables should be reliable and should be validated in real time.
Additional Information: There are several methods of ensuring that critical variables are reliably presented to the operators. These methods should be used as appropriate to achieve a high data quality and veracity. Lack of data validation places the burden of identifying valid readings on the operator. One method of achieving this, would be to have an estimate of data quality and a data quality indicator associated with each critical variable, including derived synthetic variables. Other recommended methods include: range checks for failed instruments; comparison of redundant sensors; and analytical redundancy. Range checks for failed instruments can ensure that failed instruments are identified and that they are not averaged with other, valid readings, possibly masking the failed instrument. Comparing and possible averaging redundant instruments can improve the quality and reliability of data. Analytical redundancy refers to the intercomparison of measured variables, through the use of mathematical models based upon known physical relationships among variables to determine whether there are inconsistencies in the values of the measured variables. For example, 'reactor power,' 'reactor coolant temperature rise through the reactor core,' and 'reactor coolant flow rate' are interrelated variables based upon the physical principles of heat transfer. A measured value for coolant flow should be consistent with the analytically calculated value for coolant flow derived mathematically from the corresponding measured values of reactor power and coolant temperature rise.[0800]

5.3-3 Display of Data Reliability/Validation for Critical Plant Variables

The status of the data should be displayed to the operator with an appropriate data quality indicator (e.g., valid, invalid, or unvalidated; or a derived numerical estimate).
Additional Information: Operators should also have available (e.g., on a separate display page) the individual sensor readings, so they can pinpoint an indicated problem, if the validation fails.[0800]

5.4-1 Interference with Crew Movement

The location of displays for monitoring safety parameters and functions should not interfere with the normal movement of the control room crew.

Additional Information: The display device may be located on the main control board. The displays should be accessible to the following personnel, although not necessarily at the same time: shift supervisor, senior reactor operator, reactor operator, and shift technical advisor.[0800]

5.4-2 Visual Interference with Other Controls and Displays

The display system should not interfere with visual access to other control room operating systems or with displays that are important to safe operation of the plant.[0800]

5.4-3 Labeling

Display devices for monitoring safety parameters and functions should be labeled and readily distinguished from other devices.[0800]

SECTION 6: GROUP-VIEW DISPLAY SYSTEM

6 GROUP-VIEW DISPLAY SYSTEM

Group-view display systems allow multiple personnel to simultaneously view the same information when they are in the CR or distributed throughout the plant. The most important characteristic of a group-view display is supporting team performance and not the type of device used to implement the display.

Group-view displays have traditionally been implemented in conventional control rooms using large-screen displays that enable multiple individuals to refer to the same information and allow individuals to move about the CR while still viewing the information. They can also reduce distractions that might otherwise occur if the information is needed by multiple personnel is located at the workstation of one individual. Configurations other than large-screen display devices are also used such as small-screen display devices that are conveniently located for access by multiple individuals (i.e., walkup display devices).

Conventional CRs have specific characteristics that have evolved over many years of design that contribute to crew performance. They typically feature hardwired controls and displays (and perhaps a lesser number of computer-based controls and displays) that are installed on large control panels that are shared by the crew members. Because they have fixed locations on control panels, access typically does not require unusual display-space navigation skills. Personnel who wish to use the same control or display tend to be aware of each other's intent and actions because they must share the physical devices. In addition, supervisors and other operators can often understand much about an individual's activities (e.g., which procedure step is being performed) by observing the operator's position at the control panels, which contain spatially fixed controls and displays.

Some of these positive characteristics of conventional CRs may be lost in CRs with computer-based workstations, resulting in the following types of problems:

- Difficulty maintaining awareness of overall plant status – Narrowing of attention to local problems at the expense of overall awareness has long been a problem in NPPs. This problem may be aggravated in computer-based CRs by the fact that only a portion of the total plant information is visible at one time through the limited viewing area of an information display screen.
- Difficulty and time delay associated with accessing computer-based controls and displays – Problems may result because controls and displays must be retrieved through navigation of the computer display space.
- Difficulty maintaining awareness of crew member actions – Operator actions performed in a computer-based workstation may be less identifiable when compared with actions performed at a conventional control panel. In addition, because a single control could have multiple locations in the computer display space, it may be possible for multiple operators to perform tasks involving the same control without being fully aware of each other's specific control actions and intentions.
- Difficulty communicating – Expressing ideas through face-to-face interactions using gestures or verbal communication is important to crew performance. This may be difficult in a computer-based CR because of physical separation/isolation. This problem may be further aggravated by the fact that operators have individual views of the display system and may not be viewing the same portion (e.g., display page) of the display system when they attempt to collaborate.

GROUP-VIEW DISPLAY FUNCTIONS

The overall purpose of a group-view display system can vary from design to design. The specific purpose of the system provides a basis for identifying and assessing the relevance and appropriateness of the functional capabilities and design features of a group-view display system. Some considerations to be addressed include the intended users of the system, the physical locations to be covered, the conditions

under which the system is to be used (e.g., normal operations versus emergencies), and types of support the group-view display system is to provide to personnel.

The functionality of group-view displays can include:

- Providing an overview or high-level summary of the plant status (see Section 6.1.2)
- Directing operators to additional information from other portions of the HSI by providing automatic retrieval of required information or cues to the operator to assist manual retrieval (see Section 6.1.3)
- Supporting crew coordination and awareness of each other's activities (see Section 6.1.4)
- Supporting personnel communication and collaboration for tasks such as diagnosing the cause of a process failure or performing a multi-person control task that may require discussions between personnel to coordinate information, diagnose problems, and plan corrective actions. To accomplish this a group-view display should provide information that other operators can see, discuss, and use. Verbal communication and gestures, such as pointing, are important means for communicating ideas. When operators are physically present at the same display device, communication may take the form of natural talking and gesturing. However, when operators cannot be physically present at the same display device this type of communication may take the form of computer-based interaction.(see Section 6.1.5)

USER-SYSTEM INTERACTION

The specific characteristics of group-view displays that support user interaction may be considered in two categories: (1) support for an individual's interaction with a group-view display device and (2) support for shared use of the group-view display device among multiple individuals. Each is described below.

Features that support individual interaction allow a user to access, and possibly manipulate, information presented on the group-view display. An important consideration is whether the group-view display is a stand-alone system or coordinated with the controls and displays. The following are some examples:

- Coordinated displays – The user can select options from the group-view display and the chosen items appear on a display in the user's work area.
- Coordinated controls – The user can operate both the group-view display and a display in the user's work area via the same control device such as the same keyboard or mouse.

Features for shared use allow multiple users to interact with the display. Features that manage users' access to the group-view display system are important for minimizing conflict. For example, if an individual changes the information content of the display to suit personal needs, the needs of the other crew members may not be met.

Some interaction considerations that are important to an HFE design review include the following:

- User access – Sequential user access allows one user to interact with the system at a time. This may require some sort of gate-keeping function to help users "take turns." Concurrent access allows multiple individuals to use the system at the same time.
- Control capabilities – The type of user access will affect the types of user interfaces and controls used for interacting with the system. For example, if the system is operated via cursor and has sequential user access then the cursor must be shared by the users. If the system supports concurrent use, then multiple cursors may be present on the group-view display at the same time.
- Display capabilities – Display capabilities may also be affected by the type of access. For example, if the system has a windowing capability then individual windows might be operated by different users.

6 GROUP-VIEW DISPLAY SYSTEM

Guidelines for the review of user-system interaction characteristics of group-view displays are found in Section 6.2. General guidelines for user-system interaction are found in Section 2.

INFORMATION DISPLAY

Three alternative display device configurations applicable to the implementation of group-view displays in CRs include:

- Large-screen display devices that are usually centrally located and viewable from many areas in the CR.
- Individual, redundant display devices located throughout the CR in areas where operators often work.
- Walkup display devices, within the area defined as "at the controls" by the plant's safety analysis report and technical specifications, that are not located in an operator's immediate work area.

Guidelines for the applicability of display devices are contained in Section 6.3. General guidelines for information display are presented in Section 1.

CONTROLS

The types of devices used to interact with the group-view display system should be identified, including computer-based input devices, conventional controls, and soft controls. General guidelines for computer-based input devices and conventional controls are in Section 3. Guidelines for soft controls are in Section 7.

BACKUP CAPABILITIES

If the failure or loss of availability of the group-view display system may affect operator tasks that are important to plant safety, then backup systems and capabilities should be addressed.

INTEGRATION WITH OTHER HSI ELEMENTS

The consistency and compatibility of the group-view display system with the rest of the HSI can affect operator performance and, therefore, should be addressed in the characterization. For example, the content (e.g., plant variables) and form (e.g., display formats, coding schemes) of information presented on the group-view display should be consistent with the other displays used by personnel in the CR. In addition, the user-system interaction methods used for the group-view display system should be consistent with methods used for other HSI resources.

6 GROUP-VIEW DISPLAY SYSTEM
6.1 Functional Characteristics
6.1.1 General

6.1.1-1 Applicability
Group-view displays should be used when crew performance may be enhanced by access to a common view of plant information or a means of sharing information between personnel.
Additional Information: A group-view display is one approach to presenting information and may be used to address any of the following problems:

- Difficulty maintaining awareness of overall plant status,
- Difficulty and time delay associated with accessing computer-based controls and displays,
- Difficulty maintaining awareness of crew member actions,
- Difficulty communicating.

The acceptability of a group-view display depends upon its purpose and the degree to which this purpose is accomplished. A group-view display may be considered unacceptable if it does not satisfy a recognized need or its presence detracts from personnel performance.[2090]

6.1.1-2 Group-View Display Information
Information presented in a group-view display should be relevant to the task requirements of multiple personnel and presented in a manner that is evident to its intended users.
Additional Information: Personnel should have available in their immediate work areas the information needed to perform their tasks. A group-view display located outside of the immediate work area, such as a large-screen display or a walk-up display device, should not be the sole location for information pertaining to plant conditions. Although the arrangement of information on the group-view display may be unique, the data values and status indications presented on the group-view display should also be available from the displays in the operators' work areas.[2090]

6.1.1-3 Consistency With Other Portions of the HSI
The design of group-view displays, including information presentation and interaction characteristics, should be consistent with the rest of the HSI.
Additional Information: Because group-view displays are to be used in conjunction with the rest of the HSI, consistency is necessary to support personnel in finding and using information. Guideline 1.1-17 states that consistent meanings should be assigned to codes, from one display to another. Generic HFE guidance should be tailored to specific HSIs and used to facilitate the standard and consistent application of HFE principles across the detailed design of the HSI. Since the group-view display is one part of the overall HSI, it should adhere to the same guidelines and standards of rest of the HSI, regarding such characteristics as modes of interaction, dialogue style, terminology, abbreviations, and symbols and other coding schemes. Differences should be based upon unique personnel task requirements that the group-view display is intended to support. However, obvious inconsistencies between the group-view display and the rest of the HSI, which may lead to confusion on the part of personnel, should be avoided. Examples of such inconsistencies may include presenting the same plant parameters with different units of measure or using unique coding schemes on one display device that may be confused with coding schemes used for other devices.[2090]

6.1.1-4 Control of Group-View Display
Individuals should not be permitted to make changes to the group-view display in a way that would reduce its usefulness to others.
Additional Information: Control of changes in a group-view display, such as changing variables or their ranges, may lead to misinterpretation or confusion. The use of administrative procedures is one way to control changes that may be confusing or otherwise detract from personnel performance.[2090]

6 GROUP-VIEW DISPLAY SYSTEM
6.1 Functional Characteristics
6.1.1 General

6.1.1-5 Retrieving Information via the Group-View Display
If individuals use the group-view display system to access additional information for their own use, this information should be presented on a separate display (e.g., an individual-view display).[2090]

6 GROUP-VIEW DISPLAY SYSTEM
6.1 Functional Characteristics
6.1.2 Overview Display

6.1.2-1 Providing an Overview Display
The group-view display should provide an overview display if user performance may be supported by a display that combines and integrates diverse plant data in a way that informs personnel of important conditions and allows them to see the overall status of the plant or process.
Additional Information: Operator performance may be enhanced by an overview display if:

- The demands on personnel for gathering and integrating plant data at certain times are high due to time demands from plant dynamics and competing operator tasks,
- Data needed by personnel for assessing plant conditions are dispersed within the physical space of the panels and consoles of the control room or the virtual space of the display system,
- The process for comparing and integrating data is inherently time consuming and error prone (e.g., incorrect comparisons, omissions),
- Personnel performance would benefit from rapid access to status information.

The appropriateness of overview displays should be considered within the context of the entire HSI design. The overview display is one approach to providing personnel with rapid access to important plant information. Other approaches may also be appropriate such as individual, spatially dedicated display devices. A overview display should not be provided if personnel have adequate access to required information without it and the presence of the overview display would distract personnel or interfere with their tasks.[2090]

6.1.2-2 Indicating Plant Status
The overview display should support the personnel in obtaining an overall view of plant status, gaining awareness of major changes in plant status, and identifying minor changes in plant state that are important to the plant condition.
Additional Information: The overview display should support the personnel in understanding of the immediate health of the plant during ongoing operations and response to plant upsets. It should also serve to orient people entering the control room, including during shift turnover. The overview display should indicate major changes in plant condition, such as the presence of alarm conditions. It should identify conditions that are changing, their rate of change, their significance to plant safety, and their implications for the future state of the plant. In addition, the overview display should support personnel in identifying minor changes in plant condition (e.g., changes that have not gone beyond an alarm setpoint) that are important to maintaining a general awareness of plant condition. These indications should keep personnel informed of (1) the normal operation of ongoing plant processes (e.g., closure of a valve may indicate the completion of some stage of an automatic fluid transfer process) and (2) the early stages of potential problems (e.g., parameters that are approaching alarm conditions).[2090]

6.1.2-3 Flexibility In Searching Information
The overview display should provide flexibility in the types of information searches that personnel may employ to assess plant status.
Additional Information: The overview display should support the operator in making rapid overall assessments of plant condition using various types of searches, including:

- Data driven – Searching for information that describes conditions to which personnel were specifically alerted (e.g., via alarms),
- Knowledge driven – Searching for information for which operators are specifically looking (e.g., testing hypotheses about plant status),
- Incidental – Identifying of information indicative of plant conditions for which the operator was not specifically looking (e.g., discovering potential problems while traversing the various displays in the course of other information searches or activities).[2090]

6.1.2-4 Support for Rapid Shift of View

The overview display should support personnel in rapidly shifting their focus of attention when tracking an evolving event.

Additional Information: While personnel have a tendency to focus on the details of a particular problem, the overview display should direct attention to new conditions. It should support personnel in alternating their focus of attention between the details of the event and the status of the entire plant in a manner that does not disrupt ongoing lines of reasoning.[2090]

6.1.2-5 Overall Assessment at a Glance

The manner in which information is presented in the overview display should provide a characterization of the situation as a whole in a concise form that can be recognized at a glance.

Additional Information: Rapid assessment of plant conditions requires personnel to quickly extract status information from the display. Rapid assessment is determined by both the amount of information and the manner in which it is presented. That is, presentation techniques may be used to reduce demands on the user's attention while maintaining the quantity of information contained in the display. The following design techniques are particularly relevant to the design of overview displays for supporting rapid overall assessment of plant condition:

(1) Coding schemes should be used to make important information the most perceptually salient.

(2) Related concepts should be spatially grouped and information should be imbedded within graphical objects to reduce the need for shifts in attention caused by excessive eye movement. For example, organize data by plant safety function; incorporate bar charts and digital values within symbols for major plant components.

(3) The number of objects presented should be minimized to reduce demands on short term memory.

(4) Cues that support rapid access to long-term memory stores, such as well defined object categorization schemes and pattern-matching cues, should be used to reduce demands on attention.

(5) Information processing such as filtering, suppression, and prioritization, based on considerations such as plant state and operator task requirements, should be used where the quantity of incoming information may impose excessive demands on operators.

(6) Display formats that make use of peripheral vision capabilities should only be used to facilitate non-attentive monitoring of qualitative changes of less important information and should only be implemented where they do not detract from primary task performance.[2090]

6.1.2-6 Level of Abstraction

The information presented on the overview display should be abstracted to a level that is consistent with users' information requirements for assessing plant status.

Additional Information: The overview display is intended to support personnel in monitoring and assessing changes in plant state. Information should be selected to be consistent with the types of decisions operators must make when monitoring the plant, such as determination of challenges to plant safety, the availability of plant safety systems, and the operational status of specific systems and components.[2090]

6.1.2-7 Relevant to the Viewer's Context

The overview display should present information that is relevant to activities that are ongoing and which help users determine whether events are proceeding according to expectations.[2090]

6.1.2-8 Mimic Format

The overview display should include a plant mimic when a mimic may enhance personnel performance by (1) communicating functional relationships between components or (2) providing a means of organizing information that aids information retrieval and plant monitoring.

Additional Information: Mimics are a prominent feature of overview displays for advanced control rooms. However, a mimic that is intended to provide a high-level indication of plant status may not be very informative to experienced operators because operators are very familiar with the functional relationships of the depicted systems and components. It may however, provide a useful framework for organizing plant information to support the operators in locating specific information and monitoring particular portions of the plant. A mimic format may also be valuable if it is used to depict functional relationships of lower-level components and parameters for which the operators are less familiar.[2090]

6.1.2-9 Display of Safety Parameters and Functions

If plant safety parameters and functions are presented via a combination of the overview display and other display devices, then these display devices should be within easy view of each other.

Additional Information: Plant safety parameters and functions should be displayed in accordance with the guidelines in Section 5, Safety Function and Parameter Monitoring System.[2090]

6.1.3-1 Support for Identifying Relevant Information

Where personnel performance may be enhanced by assistance in retrieving information, the group-view display should direct the user to relevant detailed information.

Additional Information: Relevant detailed information may reside in other portions of the HSI such as lower-level display screens, other display devices, and procedures to support their specific information needs. While the group-view display presents information that is of interest to the crew, it should also assist individual operators in obtaining detailed information that is relevant to their particular needs. The group-view display should provide this function if:

- The quantity of potential supporting information is high, or
- The supporting information is distributed among multiple topics/categories, or
- The supporting information is distributed among multiple information sources (e.g., display devices, procedures).[2090]

6.1.3-2 Automatic Retrieval and Presentation of Information

If information is automatically retrieved, it should be presented in a way that conveys where it came from and why it was retrieved.

Additional Information: This may be achieved using approaches such as animation in which changes in position and size of visually represented objects or concepts are used to indicate relationships.[2090]

6.1.3-3 Manual Retrieval of Information

Support provided for manual retrieval of additional information should convey the location of both the user and the additional information in relationship to the total display space and the available pathways and mechanisms for accessing this information.

Additional Information: The following are design approaches that use perceptual context to convey relationships between the locations of data in the display space and help the user develop an understanding of the organization of the data:

- Long shot view – Provide an overview (long shot view) of the structure of the display space noting current and desired locations.
- Perceptual landmarks – Provide easily discernable features that appear in successive displays that provide a frame of reference for establishing relationships.
- Display overlap – Divide a single display that is too large to be displayed at one time on a single display device into sections with some portions repeated (overlapping) between successive views.
- Spatial representation – Assign spatial attributes to data to aid human information processing(e.g., displaying data via taxonomic trees, organizing computer files using a desktop metaphor).
- System representation – Arrange the data in a manner that provides information about the structure of the process or system to which the data relates. (Woods refers to this category as spatial cognition.)[2090]

6 GROUP-VIEW DISPLAY SYSTEM
6.1 Functional Characteristics
6.1.4 Support for Crew Coordination

6.1.4-1 Support for Crew Coordination
The group-view display may be used to support crew coordination when crew performance would benefit from better awareness and coordination of actions.
Additional Information: This group-view display function consists of assisting the operators in maintaining awareness of the intentions and actions of the other operators so that separate activities can be coordinated and operators can monitor each other's activities to correct errors or promptly lend support when needed. This assistance may take many forms including providing information about operators' locations in the display system, locations in ongoing procedures, and actions performed using computer-based controls. This function is especially important in work settings where:

- Personnel need to coordinate their activities with those of others,
- The workstation design tends to isolate operators, and
- Casual observation and conversation is not adequate for maintaining awareness of others' activities.[2090]

6.1.4-2 Openness of Tools
Where enhanced coordination is desired between personnel, the group-view display should feature open tools for interacting with the HSI or the plant.
Additional Information: The "openness" of a tool refers to the degree to which it enables other personnel to infer useful information about the nature of the task and the specific actions being taken by observing its use by the operator. User interfaces that incorporate representations of physical and functional characteristics of the problem domain can provide observers with a context for understanding the task. For example, a group-view display may be used to allow personnel to observe a control action such as the alignment of a piping system. In this case, a mimic display, in which operators manipulate graphical objects, may provide more useful information to an observer than if the same task were performed via text commands on a keyboard. This is because the display conveys to the observer physical characteristics of the task, such as the type of valve being operated, and functional characteristics, such as the relationship of the valve to the overall piping system, which provides the observer with a better understanding of what action has been performed and its significance to the plant system.[2090]

6.1.4-3 Openness of Interaction
Where enhanced coordination is desired between personnel and communication is restricted by the design of the workstations, the group-view display may be used to facilitate open interactions.
Additional Information: Openness of interaction refers to the degree to which the interactions between team members allow others with relevant information to make contributions. The mode and style of interaction should allow others to see/hear the interaction and provide input (e.g., personnel working on other tasks are not excluded from providing helpful input). For example, if interactions are performed using computer-based communications or audio headsets, other crew members may not be able to observe the interaction and contribute. Where communication can be augmented visually, the group-view displays may be used to enhance the openness of interaction.[2090]

6.1.4-4 Horizon of Observation
Where enhanced coordination is desired between personnel, the group-view display should be used to allow each crew member to perceive a greater portion of the task environment.

Additional Information: Horizon of observation refers to the portion of the crew task that can be seen or heard by each individual. It is largely determined by the arrangement of the work environment (e.g., proximity of team members), the openness of interaction, and the openness of tools. By making portions of a job more observable, other team members are able to monitor for errors of intent and execution, and situations in which additional assistance may be helpful. The horizon of observation may be enhanced through the implementation of group-view displays that present information about the actions of crew members. For example, group-view displays may be used to indicate each crew member's location in the display system and the status in ongoing procedures. Group-view displays may also be used to allow personnel to monitor control actions performed by others for system anomalies or operator errors.[2090]

6.1.5-1 Supporting Communication and Coordination

Where crew performance may be enhanced by improved coordination, the group-view display may be used to support operators in actively participating in the same task through the sharing of information, ideas, and actions.

Additional Information: This function is achieved by providing the operators with a common frame of reference and tools for communication. It contrasts with the group-view function of support crew coordination, which supports personnel in coordinating separate activities. The group-view display should provide this function when:

- There is a high need for operators to work together on the same task/problem (e.g., complex diagnoses of plant failures),
- Face-to-face interaction/collaboration is difficult due to the arrangement of the work setting and the demands of concurrent tasks, and
- The quality of communication and collaboration would be enhanced by computer-based tools.
- Collaborative problem solving – Searching, retrieving, reviewing, and annotating plant information in a collaborative manner.
- Collaborative control tasks – Allowing multiple operators to perform control actions on the same plant system at the same time.
- Data recording/form filling – Entering and recording data that requires contributions from multiple operators.[2090]

6.1.5-2 General Requirements for Communication/Collaboration

If the group-view display is to be used to support communication/collaboration, it should provide a representation of the task/problem and the tools required for examining and explaining the task/problem.

Additional Information: The group-view display should provide the crew with a common understanding of the task/problem (i.e., the specific problem-solving, control, or data recording task of interest). It should provide means for crew members to express information and ideas and receive information and ideas from others regarding the task/problem.[2090]

6.1.5-3 Coordinating Input Between Participants

The group-view display should contain mechanisms to regulate the participants' access to the group-view display to allow information to be provided in an orderly manner.

Additional Information: Failure to provide regulating mechanisms may result in (1) conflict between users as they try to coordinate their presentations and (2) higher attention and processing demands for viewers as they attempt to identify contributors and process information from multiple presenters. In addition, mechanisms for regulating the participants' access should be compatible with social conventions of communication (e.g., preventing one person from monopolizing communication to the extent that it excludes all others) to allow effective use and maintain user acceptance. Any social mechanisms adopted by users for regulating the participants' access to the group-view display should support effective use of the system under a full range of plant conditions.[2090]

6.1.5-4 Minimizing Communication/Collaboration Interaction Burdens

The methods of interaction provided by a group-view display to support communication/collaboration should be designed to minimize the demands associated with executing these interactions.

Additional Information: Computer-based interfaces may impose burdens that are different from face-to-face discussions for multi-person interactions, such as providing inputs via keyboards or pointing interfaces. These burdens should not interfere with the ability of operators to interact with each other and should not detract from the operators' primary tasks associated with controlling the plant. Overall, the burdens associated with communicating and collaborating via the group-view display should be offset by the benefits gained from interactions via this media.[2090]

6.1.5-5 Compatibility With Social Conventions

The methods of interaction for communication/collaboration provided by a group-view display should be compatible with social conventions within the intended user group.

Additional Information: The design of communication/collaboration capabilities of a group-view display should be based on an understanding of social conventions within the intended user group. The communication/collaboration capabilities should be sensitive to the subtle and complex social dynamics that is inherent in group interaction. For example, by providing all individuals with equal access, the system may fail to address the special access requirements of some users (e.g., shift supervisor or TSC personnel). Also, the design of a groupware application may fail to support the use of subtle cues, such as facial and hand gestures, verbal signals, and non-verbal signals (e.g., pausing, clearing the throat), which people often use to moderate communication (e.g., indicate that they are about to start or stop talking). As another example, the system may provide capabilities for recording interactions between individuals, which may be considered unacceptable or undesirable by some users.[2090]

6.1.5-6 Flexibility in Communication/Collaboration Methods

The methods of interaction provided by the group-view displays to support communication/collaboration should be flexible enough to accommodate the range of personnel interactions that occur during normal and upset conditions.

Additional Information: The design basis for communication/collaboration capabilities of group-view displays should be based on analyses of actual interaction requirements for normal and upset conditions rather than on simplified or idealized of representations of these requirements (e.g., as depicted in operating procedures). Exception handling is critical for rapid, adaptable responses to abnormal and emergency conditions. For example, the roles of individuals in an operating crew may change from the typically roles of shift supervisor, reactor operator, and balance of plant operator, as personnel share responsibilities in response to specific plant conditions. A lack of flexibility in the group-view display for supporting this interaction may impair operator response or introduce additional workload, as operators try to find ways to work around the limitations of the system. This may detract from the operator's primary task of controlling the plant.[2090]

6.1.5-7 Identification of Participants

A coding scheme or designation system should be used to identify participants while they manipulate information on the group-view display.

Additional Information: The identification system should be developed such that it does not contribute additional clutter to the group-view display or impose excessive cognitive demands for interpretation. If participants have individual cursors, the design of these cursors should be distinctive (see Guideline 2.3.4-3).[2090]

6.1.5-8 Maintaining Historical Record of Contributions

The group-view display system should support the recording of information regarding the history of interactions if personnel tasks require this information.

Additional Information: Personnel may need information regarding the current version of an idea or the complete history, such as when an idea was introduced, who was the originator, who modified it, and when and how the idea was modified. This information should be made available.[2090]

6.1.5-9 Spatial Coordination of Inputs

When transferring information between an individual-view display and the group-view display, the information should be presented in a manner consistent with the sender's expectations.
Additional Information: When transferring information from one screen to another the user should either (1) have control over where the information will appear or (2) be informed of where it will appear (e.g., information always appears in a designated location). Transferred information should be presented in a manner that reduces the user's workload associated with finding the information and adapting to its orientation on the screen.[2090]

6.1.5-10 Timing Coordination of Inputs

When transferring information between an individual-view display and the group-view display, the information should be presented promptly and with minimal delay.
Additional Information: Response time deviations should not exceed more than one-half of the mean response time (see Guideline 2.4.3-9). When a sender transfers information to the group-view display, a lag can be an obstacle to the communication of ideas. This is especially true if other modes of communication, such as verbal, are available and lead or lag behind the group-view display. For example, comprehension may be impaired when verbal information precedes the associated visual information. In addition, problems related to participants taking turns may also result because participants are unaware that another visual presentation has started.[2090]

6.2-1 Separate Input Devices for Displays

When control of the large- and individual-view display devices is performed by separate input devices, their design should support coordinated use.

Additional Information: Problems that may result from poor coordination of multiple input devices include errors in using the wrong input device, awkward transitions between the input devices, and clutter at the operator's workstation resulting from the input devices (especially if a movable input device such as a mouse is used). The input devices should have compatible methods of operation as described in Guideline 2.3.4-4.[2090]

6.2-2 Mode Switch

When a mode switch is provided to transfer input control between the large- and individual-view display devices, protection should be provided to prevent input from being entered into the wrong display.[2090]

6.2-3 Cursor Motion

If a cursor motion is used to transfer input control between the large- and individual-view display devices, then the movement between the displays should be smooth and contiguous.

Additional Information: In this approach the desired display device is accessed by moving the cursor into the display space of a particular device. As the cursor crosses from one display device to another it should either (1) maintain continuous horizontal motion for side by side monitors, (2) maintain continuous vertical motion for stacked monitors or (3) should jump between uniquely designated locations on each screen, as described in Guideline 2.3.4-2. One should be able to follow the cursor with a simple movement of the head or eye. A combined motion such as raising and turning one's head should not be required.[2090]

6.2-4 Compensating for Different Screen Sizes and Shapes

If a cursor motion is used to transfer input control between the large- and individual-view display devices of different size and shape, then features should be incorporated to make their spatial relationships clear to the user.

Additional Information: Guideline 2.3.4-2 indicates that the cursor should jump between uniquely designated locations on each screen if the screens are not located adjacent to each other. This may be accomplished by designating a "home" or entry point on each screen. It may also be accomplished by having the smaller screen overlap with a designated portion of the larger screen (e.g., the top portion of the smaller screen may be indicated as corresponding to part of the lower section of the larger screen). Computational techniques for cursor motion, may also be used to correct for differences in the number of pixels (display elements) of the different screen sizes. For example, the upper left and right corners of the smaller display would correspond to the lower left and right corners of the larger display, respectively. When using this approach, a single movement of the cursor controller (e.g., mouse) would result in greater cursor movement on the larger screen than on the smaller screen.[2090]

6.2-5 Indicating Active Display

When using the group-view display, the user should receive a clear indication that the display is active.

Additional Information: Guideline 2.5.2-6 states that an active display window should be perceptually distinct from inactive windows. A common technique for conventional computer systems is to apply a visual code to the frame of the active window. However, for group-view displays, a multi-dimension coding mechanism is needed to indicate the status for each user because the display may be active for some operator but not for others. However, this type of coding mechanism may possibly be distracting and confusing. Thus, another approach may be to use the position of each user's cursor as a perceptually distinct cue to indicate that the group-view display is active for that user. This approach requires that the cursors be readily observable so the user can identify the display in which the cursor is present and perceptually distinct so the user can identify the cursor from those of other users. This approach may be supplemented by coding mechanisms at the user's individual-view display to indicate that the group-view display is active.[2090]

6.2-6 Processing Information to Match User Requirements

The information associated with selectable items of the group-view display item should be processed to match each user's task requirements when this processing would reduce distracting and unnecessary information and enhance operator performance.

Additional Information: One approach to supporting personnel in the retrieval of information is to have the group-view display indicate that important information is available regarding a particular topic. This may be indicated by displaying an item that individuals can select to cause the information to be presented on an individual-view display. However, the selectable item may be associated with a large amount of detailed information that may not be relevant to each individual crew member. The general principle of task compatibility states that the HSI should meet the needs and requirements of the users' tasks. Thus, the information associated with this item may be processed to better match the information to the particular user's current task requirements and eliminate information that may be unnecessary or distracting.

The processing of this information may be based on such factors as operator characteristics and plant status. These processing methods may be used separately or in combination. For example, no processing may be used for those selectable items that are associated with little supporting information, processing based on user characteristics may be used for those selectable items that are associated with large amounts of information of differing importance to individual operators, and processing based on plant status may be used when the plant enters certain configurations (e.g., after a plant trip). Another consideration is the manner in which information is made available to the operators. The alarm message processing techniques described in Section 4.1.2 and in NUREG/CR-6105, may also be applied to the retrieval of information associated via group-view displays. Finally, consideration should be given to the degree to which the operator may control or override the processing method and the availability of the information (e.g., should an operator be able to access all associated information, if desired). Use of this capability should not impose demands on the operator that detract from the operator's primary task of controlling the plant.[2090]

6.2-7 Shared Cursors

When multiple users must share a single cursor for interaction with the group-view display, features should be provided to manage access to the cursor and indicate current ownership.

Additional Information: A method of managing access to the shared cursor should be provided to prevent conflict between potential users. In addition, a distinct coding method, consistent with Guideline 2.3.1-1, should be used to indicate that the cursor is in use and to identify of the user. The use of a shared cursor may be acceptable for group-view displays that are not frequently accessed by users. Frequent use of the cursor by multiple users may impose unacceptable delays to users who require immediate information. If the group-view display is used for communication/collaboration, the requirement to take turns may impede the natural flow of information from the group, but it may also provide an implicit way of managing the input of information. Thus, the disruptions to the flow of information should be balanced against the need for information to be presented in an orderly fashion.[2090]

6.2-8 Multiple Individual Cursors

When multiple users operate individual cursors for interaction with the group-view display, a coding scheme should be provided so the users can readily identify their own cursors and identify the users of the other cursors.

Additional Information: A distinct coding method, consistent with Guideline 2.3.1-1, should be used. Individual cursors allow individuals to work independently and, thus, may be preferable to shared cursors for retrieving information from a group-view display. If the group-view display is used for communication/collaboration then additional coding schemes may be needed to indicate which cursors are active.[2090]

6.2-9 Shared Window

If the communication/collaboration function is performed by presenting information on a shared window of the group-view display, features should be incorporated to prevent new information from obscuring old information.

Additional Information: One approach to performing the communication/collaboration function is to allow users to create representations of ideas, problems, or tasks using an individual-view display and then present it to others using a window of the group-view display. A possible problem with this approach is the possible duplication of information as multiple users present slightly different versions of the same idea. This restricts the amount of information that can be added to the group-view display and adds potentially distracting clutter. A decluttering function is needed that prevents inputted windows from obscuring each other and eliminates older windows.

If the decluttering function is performed manually, it becomes a user-system interaction task that may compete with other operator tasks. If the decluttering function is performed automatically then the users may have to expend cognitive resources to locate their input when it is automatically positioned on the group-view display and adjust to changes if the decluttering function automatically removes or repositions information that is already on the group-view display. The automatic decluttering function should use techniques such as animation to help users maintain an awareness of how the content of the group-view display has changed.[2090]

6.3.1-1 Selection of Group-View Display Devices

The selection of display hardware for group-view displays should consider such factors as the user's need for immediate access to the group-view display, user's need to view the group-view display from multiple locations in the control room, ability of users to leave their usual work areas, and the type of interaction that occurs between users when viewing the displayed information.

Additional Information: The group-view display function may be implemented using a variety of display hardware. Three alternatives that are relevant to NPP control room applications are:

- Large-screen display – Large display devices that are usually centrally located and viewable from many parts of the control room.
- Individual, redundant displays – Display devices located throughout the control room in areas where operators often work.
- Walkup display – This is a smaller display device that is not located the operators' immediate work area. Operators must walk to it from their usual workstations. For example, in conventional control rooms some computer-based display devices are not located in each operator's immediate work area, but are located within a convenient walking distance. If this option is selected, the display device should be within the area defined as "at the controls" by the plant's safety analysis report and technical specifications.

Four factors that should influence the selection of the display device include:

- Need for access to the group-view display – Does the nature of the operators' tasks require them to have immediate access to the group-view display?
- Need to view the group-view display from multiple locations in the control room – Can operator performance be enhanced by viewing the group-view display information from multiple, fixed locations in the control room or while walking around the control room?
- Ability to leave usual work area to go to a walkup display – Does the nature of the operators' tasks confine them to specific locations in the control room when the group-view display may be needed?
- Type of crew interaction required – Does the use of information presented on the group-view display involve independent actions of operators, verbal communication between operators, or both verbal communication and gesturing.

Table 6.1 shows conditions under which each of the three display devices types are desirable based on these factors. A tradeoff exists between (1) the ability to use natural gesturing and (2) the other considerations such as immediate access, viewing from multiple control room locations, and ability to remain at one's usual work area. The walk-up display allows natural verbal communication with gesturing, but requires operators to gather around it. The large-screen display and redundant, small screen displays provide immediate access from each operator's work area, but the operators may be physically separated. Thus, operators may not be able to communicate using pointing and other gestures unless this capability is provided by computer-supported tools. Evaluating the acceptability of these alternatives involves consideration of the amount of time required to complete an interaction and the quality of the interaction. For example, individual interactions using computer-based tools may require more time compared to natural interactions but the computer-based interactions may be more informative and beneficial to crew performance because ideas can be expressed with more visual detail. Finally, when comparing the relative benefits of large-screen displays to redundant smaller displays, one should consider other factors such as (1) the adequacy of space for these devices and (2) the flexibility that the large-screen display provides for viewing the group-view display from multiple locations in the control room compared to the redundant smaller displays which have more restricted viewing areas.[2090]

Table 6.1 Appropriate use of group-view display devices

DISPLAY DEVICE	APPROPRIATE USE*
Large-screen displays and redundant, small-screen displays	Immediate access is required Operator must be able to view information from multiple locations in the CR Operator often cannot leave usual work area to go to a walkup display Crew interaction requirements (e.g., verbal, gesturing) are low, or computer-based communication is provided
Walk-up display	Immediate access is not required Operator does not need to view information from multiple locations in the CR Operator can leave work area to go to a walkup display

* Conditions when device is preferred.

6.3.2-1 Control of Critical Information Display

Control of large-screen group display systems should be such that critical information cannot be modified or deleted inadvertently or arbitrarily.

Additional Information: The capability to change the display should be limited to designated users who operate according to pre-established procedures, upon command of a person in charge, or both. When users must make changes that are of interest only to them, a separate, remote display (such as a console VDU) should be provided.[5908]

6.3.2-2 Maximum Viewing Distance

The determination of the maximum viewing distance on a large-screen display should be based on an analysis of the information requirements of individuals and their locations in the work area.

Additional Information: Users should be able to resolve all important display detail at the maximum viewing position; see Guideline 1.6.2-2. Application of this criterion should consider the types of information contained in the group-view display, the ways in which this information is used by individuals, and the locations of these individuals relative to the display. For example, supervisors may only need to read high-level indications from their workstations while operators may need to read more detailed information. Evaluations that use this criterion should consider the reading/viewing requirements of personnel who may be seated at the greatest distance from the large-screen display. Considerations include: (1) do the individuals need to resolve all details or merely be able to detect changes that require additional scrutiny, and (2) will some or all or the large-screen display information be available on separate displays located closer to these individuals.[2090]

6.3.2-3 Minimum Viewing Distance

The display should not be closer to any observer than half the display width or height, whichever is greater.[5908]

6.3.2-4 Off-Centerline Viewing Angle

The determination of the acceptability of off-centerline viewing should take into account both the spatial distortion of the image and the effect of the viewing angle upon screen characteristics such as brightness and color rendition.

Additional Information: Individual viewers in a fixed location should be no more than 10 degrees off the centerline. For multiple viewers, it indicates a preferred limit of 20 degrees and an acceptable limit of 30 degrees off the centerline. This guideline addresses spatial distortion of the displayed image due to the viewing angle. However, off-centerline viewing of large-screen display devices may also result in (1) loss of general brightness for high-gain screens, and (2) loss of color rendition in projection-type devices due to the angles of reflection of the separate projection elements. Loss of general brightness for high-gain screens is usually not a problem until off-centerline viewing exceeds 25 degrees for beaded screens and 30 degrees for high-gain metallic screens. These effects may further reduce perceived resolution by reducing the effectiveness of color codes and image contrast. Thus, the combined effects of off-centerline viewing upon image distortion and screen characteristics should be considered.[5908, 2090]

6.3.2-5 Viewing of Multiple Display Devices

When multiple, large display devices are used, the normal work areas of each user should be within the acceptable off-centerline viewing area of each large display that each user must view.

Additional Information: If the large display devices are adjacent to each other, they should be angled toward each other so the acceptable off-centerline viewing areas of the displays overlap. If the operators' tasks require them to work at multiple locations in the control room, the acceptable viewing area should be maximized by angling the display surfaces toward each other so that the acceptable off-centerline viewing areas of each display device coincide to the greatest extent possible.[2090]

6.3.2-6 Unobstructed View

Seating areas should be arranged to provide critical observers with unobstructed views of the display.
Additional Information: Large screen displays should be located relative to critical observers so that the view is not obscured by other people. There are two methods for achieving this: (1) laterally staggering (off-setting) personnel and consoles to maintain an unobstructed view and (2) elevating the line of sight of personnel (e.g., supervisors) who are located farther from the display so they may see over the heads of personnel located closer to the display. The line of sight may be elevated by using raised or inclined floors or by raising the height of the screen. [5908, 2090]

6.3.2-7 Externally Illuminated Displays

Externally illuminated displays should have adequate illumination.
Additional Information: Large displays that are primarily illuminated by external sources, such as static mimics, should satisfy the criteria in Section 12.1.2.3 for illumination, uniformity, task area illumination, shadowing, glare, reflectance, and color. The level of illumination should provide adequate contrast to allow users to resolve all important displayed details at the maximum viewing distance.[2090]

6.3.2-8 Projected Displays

The optical characteristics of projection systems should conform to the guidelines given in Section 1.6.2.[2090]

6.3.2-9 Text Size

The size of text for labels and detailed information should be based on analyses of the maximum viewing distances of personnel.
Additional Information: The height of letters and numerals should typically not subtend less than 15 minutes of visual angle as measured at the maximum viewing distance; see Guideline 1.6.2-3. However, the maximum viewing distance may be different for different types of information in the display. For example, labels and high-level status indications may require larger viewing distances (e.g., across the control room) while individual parameter values may require shorter viewing distances (e.g., must be legible from panels that contain the corresponding controls). Therefore, the determination of acceptable text size should consider the type of information and the context in which it will be used.[2090]

6.3.2-10 Use of Labels

The presence of labels should not cause excessive clutter or detract from detailed information.
Additional Information: Because labels may be large and may require large separations (Guideline 1.3.3-6), they tend to clutter large displays. The EPRI URD requirements for the MCR Integrating Display and Mimic state, "Labels which are to be read at a distance shall be minimized; however, when the display is viewed from close range, each display quantity should be specifically identified by a label readable at the short distance." The need for labels may be reduced if graphical means such as mimics and symbols are used to identify information.[2090]

6.3.2-11 Use of Information Displays Developed for Standard Video Display Units (VDUs)

Displays developed for standard VDUs should not be presented on large-screen display systems without first being evaluated for acceptability.

Additional Information: Large-screen display devices tend to have lower brightness and resolution than standard VDUs and are susceptible to glare from ambient light sources. This may result in reduced legibility and reduced effectiveness of color coding schemes. Text, graphics, and color codes should be reviewed and adjusted to suit the characteristics of the particular display device.[2090]

SECTION 7: SOFT CONTROL SYSTEM

7 SOFT CONTROL SYSTEM

The basic function of soft control systems is to provide operators with control interfaces that are mediated by software rather than by direct physical connections. Soft controls can be used to control plant equipment, such as a pump, or the HSI itself, such as display selection. The unique characteristics of soft control systems that make them different from conventional controls, e.g., hardware knobs and buttons, are described below.

Spatial dedication vs virtual location – A conventional control typically has a unique location in the CR and is used to control a specific aspect of the plant or HSI. By contrast, a soft control for the same function is typically not spatially dedicated and may exist in multiple locations, e.g., it may be accessed from more than one display device, and from multiple pages within a display device. Thus, soft controls often lack the degree of spatial dedication that is characteristic of conventional controls.

Serial versus parallel presentation – Conventional controls are presented in parallel; i.e., all controls exist in their spatially dedicated location at the same time. Operators visually scan the controls to determine their status. Computer-based HSI components usually contain more displays and controls than can be viewed at one time via its display devices. Because the total set of displays cannot be viewed at once, the user views portions of it one after another, similar to a person looking into a room through a keyhole in a door. This 'keyhole effect' limits the number of soft controls that can be viewed or used at one time, thus forcing serial rather than parallel access.

Present versus available – Conventional controls are spatially dedicated and as such are continuously present in the control room. Soft controls may either be designed to be continuously present like conventional controls, or they may have to be retrieved from a display system. Hence, soft controls may be considered available but not necessarily present. In addition, the availability of soft controls can be restricted to specific conditions. For example, some soft controls, such as those used for configuring digital control systems, may have protective features (e.g., password protection) that limit their availability to specific personnel or situations.

Physical decoupling of input and display interfaces – Typically, conventional controls are located close to their associated display. That is, operators perform the input actions and monitor feedback at the same location (e.g., when turning a rotary dial, the operator observes its motion and reads the new setting from its perimeter). For soft controls, there may be a looser physical coupling between the location of control action and the presentation of feedback. That is, the operator may take a control action in one place and read the setting elsewhere. For example, when using a pointing interface, the user may manipulate a mouse on a console top to move a cursor across a display screen to select an icon. The results of this action may be displayed in yet another location, such as a window indicating that some equipment has been turned off or on. In this case, the operator must monitor three locations to complete a single control action: the mouse, the icon, and the window. This physical decoupling of the input device (e.g., the mouse) and the displays that present feedback may result in monitoring demands that differ from conventional controls.

Plant control versus interface management control – Actions that control the HSI (i.e., cause displays to be presented) can be distinguished from actions that control the plant. Both types of actions may be performed using the same or different input and display devices. For example, an operator may use a mouse and VDU to access a display and then use the same mouse and VDU to operate a piece of plant equipment (e.g., a pump) from that display. In this case, the mouse and VDU are used to operate both the HSI and the plant.

Multiple modes – While a conventional control typically performs a single control function, a soft control may perform a range of control functions, each representing a different mode (e.g., mode 1 for performing function A, and mode 2 for performing function B). The behavior of these functions is defined by the

software. Options for control actions are usually communicated to the operator via displays. When the operator carries out a control action, the software converts the results into a signal for the control system. Hence, a specific action, such as pressing a button, can produce different results depending on such factors as the particular display page currently accessed, the status of the control system, and the status of the plant.

Complex control functions – Because the operator's actions are interpreted by software, many operations may be initiated via a single action using a soft control. For example, a sequence of operations required to start plant equipment may be linked to a single "Start" command. While conventional control systems also offer this capability (e.g., via relays), software-defined functions can result in more complex linkages among operations.

Interface flexibility – Computer-based technology can allow the user interface of soft controls to be adaptable to changing needs or conditions of use. For example, the operator may be able to arrange the presentation of the control and its associated information based on a current need or personal preference. Alternatively, the control and information may be automatically arranged based on the current situation.

INFORMATION DISPLAY

Information display considerations important to operator performance using soft control systems include the means for selecting the components to be controlled, the display areas where input is entered, and the formats used for entering data. Each of these is described below. General review guidelines for soft control displays are given in Section 7.2.1. The general display characteristics of soft controls should also be reviewed using Section 1, Information Display.

Selection Displays

These are displays used when choosing the variables or plant components to be controlled. Two commonly used formats are the mimic and the list. Review guidelines for selection displays are provided in Section 7.2.2.

Input Fields

These are display areas used for providing input (e.g., entering a new control setpoint). Input fields may appear on an adjacent display device, as a window placed on top of a selection display, or as a data entry field inside a control selection display. Review guidelines for input fields are provided in Section 7.2.3.

Input Formats

These are formats used for entering data. Important characteristics include the representation of formats commonly used with soft control systems (e.g., discrete-adjustment interfaces, soft sliders, and arrow buttons). Review guidelines for input formats are provided in Section 7.2.4.

Display Devices

The display devices on which soft control systems are presented may be either functionally dedicated or general purpose. A functionally dedicated display device is used for a specific function or set of functions (e.g., a display device used only to interact with a particular plant system, such as feedwater control). A general-purpose display device may be used to interact with a broad range of plant systems. This distinction affects where a soft control may be accessed in the HSI and, possibly, the degree of interaction required to access it. For example, if a soft control can be accessed from a set of general-purpose display devices, then it may be accessed from multiple locations in the control room, but a high degree of interface management may be required to retrieve it from the other displays in the network. Conversely, a display device dedicated to a small set of plant variables may require very little interface management to

access the desired soft control. A variety of VDU hardware may be used to present soft controls. Review guidelines for display devices are presented in Section 7.2.5.

USER-SYSTEM INTERACTION

Interactions with soft controls include selecting a plant variable or component to be controlled, providing the control input, and monitoring the system's response. Each is described below. In addition, system response characteristics are also described.

Selecting Plant Variables or Components

A separate step is often required to select the specific plant variable or component that is to be controlled by a soft control. Selection methods may require the user to make a choice from a set of options or to identify a choice from memory. The following interaction methods are commonly used to present the operator with a set of options.

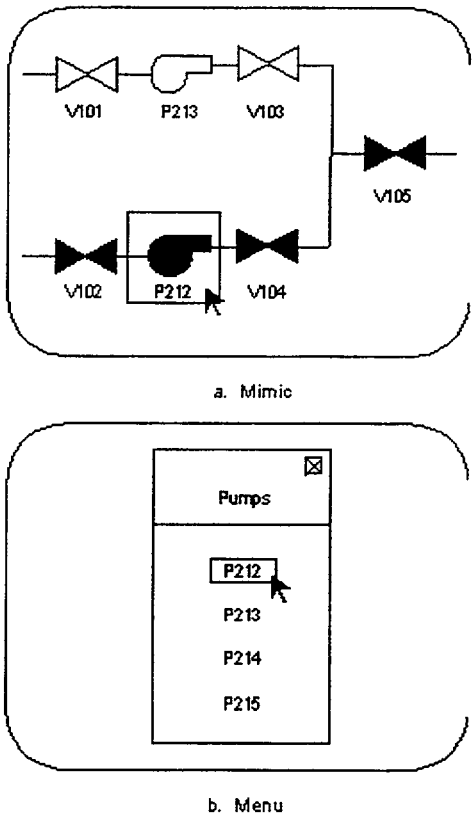


Figure 7.A Two typical displays for selecting variables or components (with on-screen cursor)

Mimic display – Typically, plant components are represented by symbols, and the flow paths (e.g., for mass or energy) are represented by lines. Operators may select a component from a mimic display by using a pointing device. Alternatively, the operator may use a keyboard to enter the identification code for the specific component. The top part of Figure 7.A depicts a component being selected from a mimic display through the use of a cursor.

Menu display – This is a display format that shows a list of alternatives. Selection may be made using a pointing device, function key, or by using a keyboard to enter an identification code. The bottom part of Figure 7.A depicts a component being selected from a menu display through the use of a cursor.

Dedicated button – This is a button whose activation will cause a particular control or display to be retrieved. It may be dedicated to particular soft control. A dedicated button may be a physical 'hard' button located on a keyboard of console or a 'soft' button presented on a computer-based display device.

The following interaction methods generally require the user to identify a choice from memory: command language, natural language, query language, and question and answer dialogues. These methods may be augmented with online forms and other aids to help the operator compose entries. Input is typically provided via alphanumeric keyboards. However, other input mediums, such as voice, are also possible.

Providing Control Inputs

Providing control inputs often requires at least two steps: accessing the input field and providing control inputs. Input fields are areas of the display where users enter values for the control system. These areas may be part of the display used to select the plant component or variable, they may be displayed as a window on that display, or they may be displayed on a separate device. When the input field is integrated into the display, the user provides input directly, e.g., an operator may open or close a valve by clicking on its icon. No additional adjustment of the display screen may be necessary because no new input window is introduced. An example is shown in Figure 7.B. When the input field is window, selection of a component or variable causes a window to appear to accept input. For example, an operator may select a component from a mimic display by clicking on it with a mouse. This causes an input window to be positioned in the display. The display may have a space dedicated to the input window or the window may be superimposed on the display and overlap or obstruct part of it. An example is shown in Figure 7.C. When the input field appears on the screen of a separate display device, the interaction is similar. For example, an operator may select a component from a mimic display by clicking on it with a mouse. This causes the input field to appear on an adjacent display device, allowing the input field to appear without obstructing the user's view of the selection display. An example is shown in Figure 7.D.

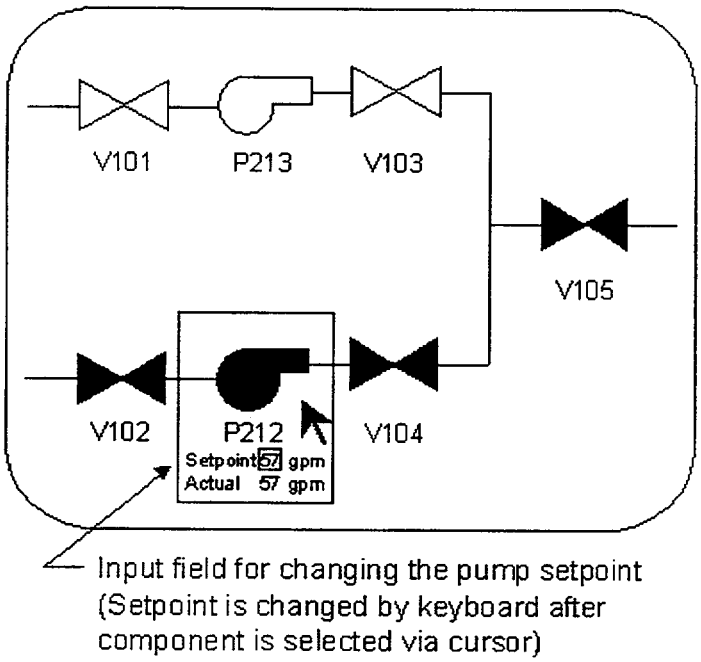


Figure 7.B Soft control input field is integral with selection display

The input field configurations in Figures 7.C and 7.D are more commonly used in process control applications than the integral configuration shown in Figure 7.B. This is because they provide more space for displaying setpoints and other related values.

Once an input field has been accessed, three categories of inputs can be provided to affect the state of the plant: command inputs, discrete values, and continuous values. Each is described below.

A command is an instruction to a computer or system requesting it to perform an action. For example, commands may be given to obtain, transfer, process, store, retrieve, delete, or display information about plant status. Commands may also be used to control the plant (e.g., as an instruction to an automatic control system to perform a function, such as shutting down a piece of equipment).

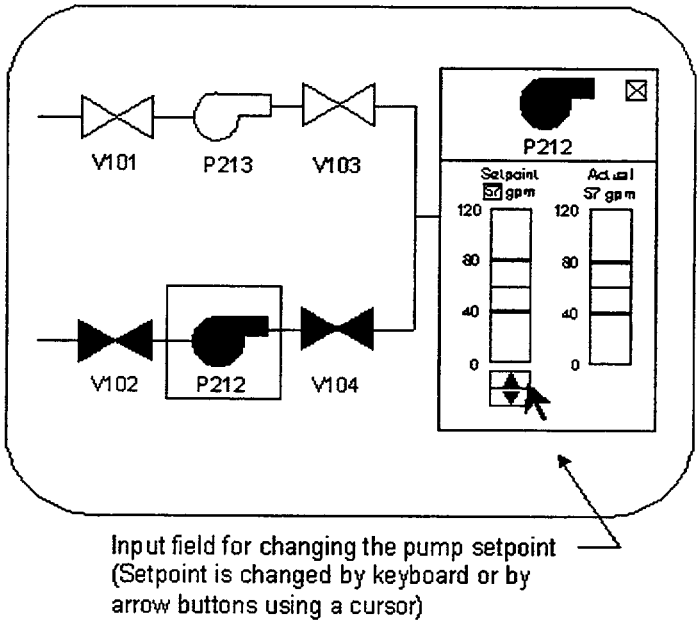
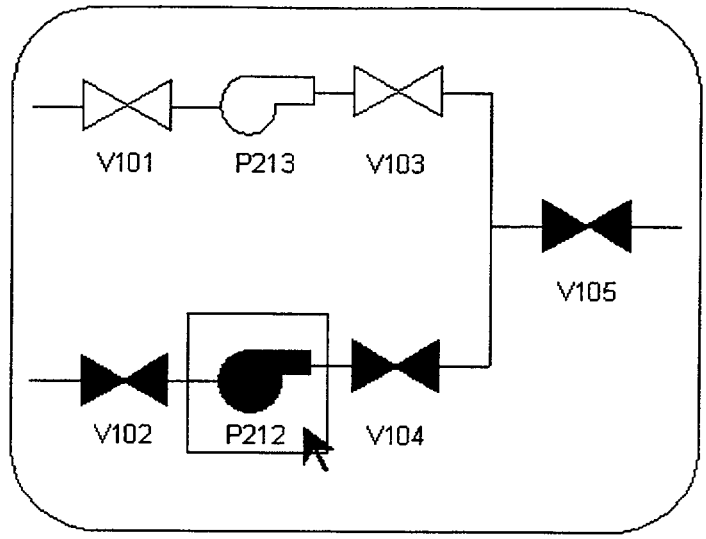


Figure 7.C Soft control input field is a window within the selection display

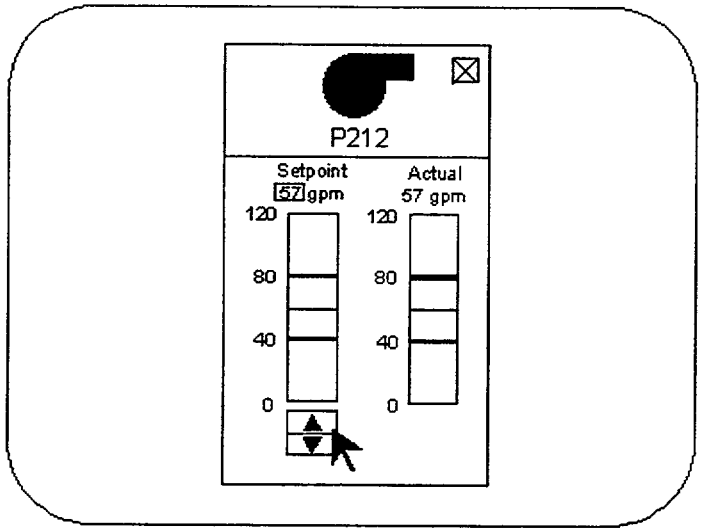
A discrete variable has a defined set of individual values. The input action involves selecting one of them. Many control actions involve making a selection from a discrete set of states. For example, plant breakers and valves may be changed from the open to the closed state.

Automatic controllers have discrete control modes (e.g., manual, automatic, and cascade). In addition, controls used for interface management may have discrete settings. For example, buttons may be pushed to access particular displays. Input formats used for providing discrete-variable inputs may be referred to as discrete-adjustment interfaces; they have individual settings that can usually be accessed with fairly gross movements. Their operation is similar to physical controls that provide discrete adjustment, such as push buttons and switches.

A continuous variable has a continuous set of values within a defined range. Many control actions involve providing a value from a continuous range, e.g., when changing a control setpoint, the operator increases or decreases the setting of a controller within a defined range. When using physical control devices, continuous variables are often set using continuous-adjustment controls. The desired value is accessed using some type of slewing motion requiring a gross movement followed by a fine adjustment. With soft controls, continuous variables may be adjusted in a variety of ways. Three common means are described below.



Selection Display



Input Field Display

Figure 7.D Soft control input field and selection display are on separate display devices

First, incremental input devices may allow continuous-adjustment such that the position of the device corresponds to the magnitude of the input value. These are similar to continuous-adjustment control devices, such as dials, levers, and sliders. For example, the magnitude of input provided by a dial corresponds to the degree to which it is rotated. A large change in a value requires a large degree of rotation of the dial from its current position. An example is the soft slider (i.e., a slider presented on a computer-based display device), which resembles a bar chart with a pointer directed toward the current value. Input is accomplished by sliding the pointer via a mouse or touch screen interface along the length of the bar chart scale to the desired value.

Second, incremental input devices may accept discrete inputs that change the variable by a specific amount. One example is a pair of buttons pointing in opposite directions that are used to increase and decrease a value sequentially. Arrow buttons may be implemented on a display screen or on a keyboard. Soft buttons are typically presented on the display screen and operated via a pointing device, such as a mouse or touch screen. Hard buttons may be physical keys mounted on a keyboard or panel that are used in conjunction with a display screen. With each press of the increase button, the variable increases by a specific amount. If the button is held down, the variable will increase in proportion to the length of time that the button is depressed.

A common design practice is to have the input value change by the smallest unit of precision presented by the soft control device for each press of the arrow button. For example, if the soft control presents a variable to one decimal place, then one press of the arrow button will change the value by one tenth (e.g., increase the value from 10.1 to 10.2). If the variable is presented in integer values, then one button press will change the current value to the next integer (e.g., increase the value from 11 to 12). If a variable has a wide range, executing a large change in the value may require pressing the button many times or holding it down for a long time. Some soft controls feature a second set of arrow buttons that can change the input value by a larger amount for each button press. For example, single arrow buttons [>] may be used for making small changes and double arrow [>>] buttons for making large ones. The size of the increment provided by the double arrow buttons may be configured by the control system engineer for each soft control. The standard values provided by the vendor for the double arrow buttons are 2%, 3%, 5%, or 10% of the range of the instrument. Other values may be programmed.

In some computer-based control systems, the size of the increment provided by incremental input devices may change as a function of plant or system state. For example, a single press may produce a large change during plant startup but a small change when the plant is in its normal operating range.

Finally, keyboards and number pads may be used to enter values in digital form using a set of key actuations, e.g., the value '100.7.'

Several formats may be combined in a single soft control.

Monitoring Control Feedback

Control feedback refers to indications provided to the user that show whether the user's entry was accepted by the system, whether the system is responding to the input, and whether the input is having the desired effect. Each is described below.

System Acceptance Feedback

System acceptance refers to feedback that indicates whether the user correctly performed the input action. For example, when an operator provides an input, an indication is given to show whether the user interface was manipulated properly. Feedback may entail visual cues, such as computer-based buttons that change color when selected, and auditory cues, such as a click accompanying a selection. The system should also provide feedback indicating whether the user's entry was acceptable. For example, if the user enters a value that is outside of acceptable range or selects an unacceptable command, the system should alert the user by visual cues (e.g., changes in symbols to indicate that the user entry is not acceptable or that the selected option is not available), warning messages (e.g., a description of the problem), or auditory tones (e.g., a tone that directs the user's attention to the problem). The soft control should also display the user's entry in a way that allows the user to review it and determine whether it is correct. A variety of text and graphical approaches can be used. For example, when the operator enters a control setpoint, the value may be presented in text format by displaying the digits via the user interface. The setpoint may also be represented graphically. One commonly used format is the bar chart. The bar is usually depicted against a reference scale with its length or height corresponding to the magnitude of the

input value. Text and graphic feedback may be combined. For example, the input value may be depicted in both digital and bar chart formats.

System Response Feedback

System response feedback indicates whether the user's entry, which was accepted by the system, is being acted upon. For example, an operator may use a soft control to operate a pump by entering a new (higher) control setpoint for pump speed. After providing acceptance feedback indicating that the new setpoint was within the acceptable range, the soft control should provide system response feedback indicating whether the pump is responding to the new setpoint. That is, the operator should be able to determine whether the speed of the pump is increasing toward the setpoint value. To provide this type of feedback, the soft control should be coordinated with plant displays that indicate system status.

Goal Achievement Feedback

Goal achievement refers to feedback that indicates whether the input is achieving its intended goal (e.g., moving the plant toward a safer state). For plant control actions, such as adjusting the flow rate of a feedwater pump, it is necessary that the operator determine that the intended goal (e.g., increased steam generator level) is achieved. To provide this type of feedback, the soft control should be coordinated with plant displays that indicate system and plant status. For example, mimic displays can support the operator in selecting plant components, monitoring the system's response, and monitoring goal achievement. When selection displays and input fields are implemented in other ways, such as via menus and tables, respectively, the higher-level goals affected by the control action may not be readily visible.

System Response Time

Total system response time may be described as the time between the submission of an input to the soft control system and the various types of feedback. For soft controls, system response time may affect the ability of operators to control the plant. Four response time factors are described below.

Display retrieval time is the time required for the HSI to present a new display following the onset of a command. For soft controls, this includes the time required to retrieve: (1) a selection display, and (2) the input field with which operators provide input. Slow response time for retrieving displays can delay the operators' access to important information.

Display update time is the interval with which plant variables shown in the soft control or associated displays are updated with new data. If the update rate is slow relative to the behavior of the plant, then a soft control or display could present data that is not representative of the current state of the plant.

Sampling rate and interval for inputs is the number of scans of an input field per unit of time. The sampling interval is the amount of time between samples. Computer-based display systems typically scan the input fields for new input from the operator. If the sampling interval is large, then a long delay could exist between when an input is entered and when it is received by the control system.

Plant response time is the interval between the time at which an input is received by the control system and the plant achieves the desired state. It may have two components: (1) response time for the plant system (i.e., the time required for plant equipment to respond, such as an electrical breaker closing) and (2) response time for the plant process (i.e., the time required for the plant process to achieve the desired goal state, such as reaching a target temperature value). These response times can be fast or slow. If the response is slow then the operator may have difficulty determining whether an input value was too high or too low. As a result, the process value may overshoot or undershoot the target value. If the response time is fast, the operator may lack sufficient time to recognize and respond to input errors.

These response times, combined with operator response time, determine the overall response of the human-machine system. For example, the total time required to access a particular display is the sum of the time required for the operator to select the display and the HSI to respond (display retrieval time). The

total time required for achieve a desired change in plant state is equal to the sum of the time required for the operator to enter the input value, the HSI to sample the input value, the plant to respond to the input, and the HSI to represent the change in a display.

CONTROLS

Soft controls are implemented using a broad range of input devices, including those presented in Section 3; thus, no unique guidance is provided for soft control input devices. In addition, conventional, hardwired control devices may also be used if their operation is interpreted by software (e.g., to access multiple plant variables). For example, a physical pushbutton located next to a display screen could perform several different functions depending upon the information presented in the display screen. Finally, soft control systems may also be operated via speech input; review guidelines for speech input are provided in Section 2.2.10.

BACKUP CAPABILITIES

If the failure or loss of availability of the soft control system may affect operator tasks that are important to plant safety, then backup systems should be addressed. For example, a separate set of conventional controls may be provided as an emergency backup for controls that are important to plant safety.

INTEGRATION WITH OTHER HSI ELEMENTS

The consistency and compatibility of the soft control system with the rest of the HSI can affect operator performance. Thus, important review considerations include the degree to which the control devices and displays of the soft control system are compatible with other controls and displays of the HSI.

7 SOFT CONTROL SYSTEM

7.1 General

7.1-1 Coordinating Soft Control Use Among Operators

If a soft control can be accessed from more than one location in the HSI, protective measures should ensure its coordinated use among multiple users.

Additional Information: The HSI should be designed to allow operators to maintain awareness of each other's use of the soft control so their actions do not interfere. For example, two operators should not be able to operate the same soft control simultaneously from different places without being aware of each other's actions. Coordination problems may be minimized by assigning the control capability for a soft control to a particular individual or workstation (e.g., while the settings of a soft control can be viewed from multiple display devices, it can only be operated from one device). Alternatively, coordination may be supported by features that restrict access to soft controls one user at a time, and group-view displays that allow operators to observe each other's actions.[6635]

7.1-2 Operation with Protective Clothing

Soft controls should be designed to accommodate any protective clothing that personnel may be required to wear.

Additional Information: In some plant locations, environmental conditions necessitate wearing protective clothing that can limit the ability of personnel to manipulate soft controls. For example, gloves may reduce manual dexterity and tactile sensitivity, degrading the ability of personnel to operate soft controls quickly and accurately. As another example, eye protection, such as goggles, may become foggy or distort vision and, thus, interfere personnel's ability to view computer-based display devices.[6635]

7.2.1-1 Representing Relationships Between Control System Components

The display capabilities of soft controls should allow users to quickly assess the status of individual components of a control system and their relationships with other components.

Additional Information: Due to the limited size of the display devices used with soft controls, not all components of a control system may be visible to the operator at once. However, they should allow the operator to rapidly view relationships between functionally related components. For example, if a controller is part of a hierarchical control system, the operator should be able to see higher-level controllers that provide control inputs and lower-level ones that receive inputs. Rapid assessment of the control system's status should be supported by such features as displays that depict these relationships, and retrieval mechanisms that give rapid access to detailed information on individual control system components.[6635]

7.2.1-2 Making Options Distinct

The interface should be designed so that users can, at a glance, distinguish options by such characteristics as context, visually distinct formats, and separation.

Additional Information: Slips involve errors in performing well-practiced, unconscious actions. Description errors, a type of slip, involve performing the wrong set of well-practiced actions for the situation. They occur when the information that activates or triggers the action is either ambiguous or undetected. Many control input actions involve the selection of options, such as choosing between alternative commands or selecting a plant component to perform a control action upon it. Description errors that result in selecting a similar but incorrect option may be prevented by organizing options to supply context (such as by functional organization), making options visually distinct, and separating options that users may confuse. Options may be separated by placing them on different display pages or different display devices.[6635]

7.2.2-1 Visually Distinct Selection Displays

Displays used for selecting components and variables should be visually distinct to support choice of the correct display.

Additional Information: A selection display shows a set of components or variables that may be chosen for a control action. One common format is the mimic, in which components are arranged as a schematic diagram. Excessive reuse of layouts and display elements in mimic displays may cause them to look alike and so may contribute to operators searching the wrong selection display for the component that they wish to manipulate. Selection displays should be laid out and labeled so operators readily recognize and distinguish them.[6635]

7.2.2-2 Visually Distinct Components

The representation of components and variables within selection displays should be visually distinct to support their correct selection.

Additional Information: Using a standard set of symbols and layout conventions in displays is important in reducing the mental workload associated with finding and interpreting information. However, these factors may also cause components to look alike and may contribute to operators selecting the wrong component. The symbols and graphical icons used to represent different types of components should be designed to be readily recognized and distinguished. In addition, they should be clearly labeled for correct identification.[6635]

7.2.2-3 Identification of Loops on Multiple-Loop Controllers

The loops of multiple-loop controls should be distinctly marked to prevent the selection or use of the wrong loop.

Additional Information: A multiple-loop controller is a digital controller that can control multiple variables via independent channels, one per control loop. Each channel acts as a separate control device. For example, a single controller may be capable of controlling 10 different variables, each on a separate control loop. Operators access these loops through the user interface of the controller device. However, because there may be few cues to identify the loops, operators may fail to correctly recognize the loop accessed and may control the wrong variable.[6635]

7.2.3-1 Cues for Matching Input Fields to Selection Displays

A user looking at the field for providing a control input should be able to determine which plant component or variable is being controlled.

Additional Information: The design of a soft control should provide a salient link between the input field and the corresponding variable or component. Starting at the input field, the operator should be able to quickly trace the component or variable back to its representation in the display that was used to select it. Three methods that might be used are graphic coding, landmarks, and animation. Graphic codes, such as borders, symbols, and colors, may be applied to both the representation of the component in the display from which it was selected and to the input field, making a strong visual association between them. For example, if the selection display has a mimic format, the input field may contain the symbol for the selected component. It also may contain symbols for the components that precede and follow it in the flow path. Animation may be used when an input field is opened and closed. The input field could appear as if it were 'popping out' of an option selected from a display, and 'go back' into the option when the field is closed.[6635]

7.2.3-2 Labeling of Input Fields

The input field should be labeled with sufficient information to uniquely identify its corresponding component.

Additional Information: Labeling should include a unique identification code for the component, matching its representation in the selection display. It may also describe the component (e.g., valve, pump, breaker) and identify those components that immediately precede and follow it in the system.[6635]

7.2.3-3 Coordination of Soft Controls with Process Displays

Displays should be readily accessible from the input field so the user can readily verify that the control actions have had the intended effect on plant systems and processes.

Additional Information: Inadequate coordination of input fields with plant process displays can make it difficult for operators to verify that control actions have had the desired effects on plant systems and processes.[6635]

7.2.4-1 Appropriate Use of Discrete-Adjustment Interfaces

Discrete-adjustment interfaces should be used for selecting among a set of individual settings or values.
Additional Information: Discrete-adjustment interfaces are computer-based formats with individual settings that can be accessed by fairly gross movements; their operation is similar to discrete-adjustment controls, such as push buttons. By contrast, continuous-adjustment interfaces are computer-based formats that have continuous ranges usually accessed using some type of slewing motion, requiring a gross movement followed by a fine adjustment; their operation is similar to that of continuous-adjustment controls, such as rotary dials or sliders. Discrete-adjustment interfaces are preferred when the user must select one option from a limited number of choices, or when precision requirements are such that a limited number of settings can represent the entire continuum of values. The most common discrete-adjustment interfaces used with soft controls are individual buttons and radio buttons (a group of buttons representing a set of related options). However, other formats also are possible, such as rotary selector dials operated via cursor or gestural interfaces. Some computer interfaces have a continuous-adjustment control, such as a slider or scroll bar, for looking at a group of individual options. Because choosing a specific setting with a continuous-adjustment control can be awkward, there should also be a discrete-adjustment control, such as a set of arrow buttons.[6635]

7.2.4-2 Labeling Selection Options in Discrete-Adjustment Interfaces

The selection options in discrete input formats should be clearly labeled.[6635]

7.2.4-3 Feedback for Discrete-Adjustment Interface with Multiple Settings

Discrete-adjustment interfaces should indicate which setting was selected.[6635]

7.2.4-4 Feedback for Discrete-Adjustment Interface with Continuous Operation

If a discrete-adjustment interface has continuous operation, it should provide continuous feedback on the current state.
Additional Information: A continuous-operation control continues to produce an effect until the user provides the next input, or until a predefined action sequence is stopped by a termination criterion. An example is a button that changes to the activated state when pressed and remains in that state until it is pressed again. An example of continuous feedback in a soft control is a checkbox format in which an 'X' appears in the box to indicate that an option has been selected, and disappears only after the option is de-selected.[6635]

7.2.4-5 Appropriate Use of Continuous-Adjustment Interfaces

Continuous-adjustment interfaces should be used when precise adjustments along a continuum are needed or when many discrete settings are present.
Additional Information: Continuous-adjustment interfaces, such as soft sliders, provide continuous adjustment and are, therefore, suited to selecting a setting from a continuum. Because these interfaces often require a gross slewing movement followed by fine adjustment, setting them correctly may require more time and attention than discrete input formats. Therefore, they should not be used in place of a discrete-adjustment interface for selecting from a small set of options.[6635]

7.2.4-6 Appropriate Use of Soft Sliders

A soft slider should be considered as an input device when the range of possible values and the ratio of a value to that range need to be displayed.

Additional Information: A soft slider (also called a slider bar or a scroll bar) is an input format used to directly manipulate a variable over a set range of values. Soft sliders are typically maneuvered via pointing interfaces, such as a touch screen or mouse. They may require careful hand-eye coordination to ensure that the pointing device does not leave the linear path of the slider nor overshoot or undershoot the intended target. If the user's tasks do not permit careful hand-eye coordination, then other interfaces, such as arrow keys, should be used. The slider sometimes is combined with arrow buttons.[6635]

7.2.4-7 Indicating the Range of Values on Soft Sliders

The range of values should be indicated on horizontal sliders with the low value on the left and the high value on the right, and on vertical sliders with the low value on the bottom and the high value on the top.[6635]

7.2.4-8 Displaying the Digital Value on Soft Sliders

The numerical value to which a soft slider is set should be presented in digits on the soft slider.[6635]

7.2.4-9 Dimensions of Soft Sliders

The physical dimensions of the soft slider should allow the user to read the current and target positions and position the slider with the required precision, accuracy, and response time.
Additional Information: The length of the slider is determined, in part, by the range of values depicted, the increments between individual values, the degree of precision required for reading the slider's position, and the user's expected viewing distance. The accuracy with which the slider may be positioned may be affected by characteristics of the input device (e.g., mouse devices may allow more accurate positioning than a touch interface due to the size and irregular shape of the finger). A very short slider may be difficult to read or position precisely. A very long slider may produce slow response times due to the long distance that must be traveled and the need to keep the pointing device on its linear path.[6635]

7.2.4-10 Depicting Critical Ranges on Soft Sliders

When part of the range of values depicted by a soft slider represents critical information, such as alarm limits, those values should be coded to facilitate recognition.
Additional Information: Graphical codes may be applied to distinguish the normal operating range, alarm limits, and other abnormal operating ranges.[6635]

7.2.4-11 Appropriate Use of Arrow Buttons

A set of arrow buttons should be considered as the input device when it is desirable to incrementally increase or decrease a variable from its previous value.
Additional Information: Arrow buttons change values sequentially as each increase or decrease button is pressed. In addition, values may change continuously if a button is held down. These inputs provide feedback about the magnitude of the change (i.e., the magnitude increases with the number of presses or the time that a button is held down). Such feedback may reduce the likelihood of producing large errors or increase the likelihood of detecting them. Some soft controls have two sets of arrow buttons, one for small and one for large incremental changes. Arrow buttons are sometimes combined with a slider in a soft control.[6635]

7.2.4-12 Indicating Current Value for Arrow Buttons

Arrow buttons should have a display indicating the current value of the variable being controlled.
Additional Information: The current value should be shown in a format consistent with the type of variable being controlled. Numerical values should be presented as digits, and textual values (e.g., Low, Medium, and High) as words.[6635]

7.2.4-13 Uniform Changes in Values Via Arrow Buttons

Each press of an arrow button should change the current value uniformly.[6635]

7.2.4-14 Feedback Regarding Arrow Button Actuation

Arrow buttons should provide salient feedback when they are actuated.
Additional Information: Feedback should be sustained when the button is held down and momentary when the button is momentarily pressed.[6635]

7.2.4-15 Apparent Operation of Arrow Buttons

Labeling and other coding should be used when the operation of the arrow buttons is not apparent.
Additional Information: For example, when arrow buttons are used to change a date display, it may be unclear whether actuating a button will incrementally change the days (and change the month when the last day is reached), or whether the month and day values are changed separately after being selected by the user. The arrow buttons should be labeled or coded to indicate their effects.[6635]

7.2.4-16 Reference Values For Continuous Variable Inputs

Reference values should be provided to help the user judge the appropriateness of values when entering continuous variable inputs.
Additional Information: Reference values commonly used in process control applications include the variable's range, alarm limits, and the current value. Reference values may be presented as digits or graphs.[6635]

7.2.5-1 Adequate Display Area

Adequate display space should be provided so that short-term monitoring and control tasks do not interfere with longer-term tasks.

Additional Information: Making control actions available via a general-purpose display device may require other plant information to be removed from the user's view. Sufficient general-purpose display devices should be provided so that short-term control actions can be undertaken without interfering with long-term ones (e.g., they can be performed on separate devices). Alternatively, control actions can be supported by dedicated special devices.[6635]

7.3.1-1 Minimizing Soft Control Modes

The excessive use of modes in soft controls should be avoided.

Additional Information: Modes occur in soft controls when a display or input device is designed for more than one function. For example, a soft control that is used for manipulating multiple variables may have a separate mode for each one (e.g., individual modes for variables A, B, and C). In addition, there may be multiple modes for a single variable, each allowing it to be controlled in a different way (e.g., variable A may have separate modes for manual control, automatic control, and testing). Mode errors occur when the user believes the device is in one mode when it is in another and, as a result, performs an inappropriate input action. The likelihood of mode errors can be lessened by reducing the number of modes; if multiple modes do not exist, then mode errors cannot occur.[6635]

7.3.1-2 Distinctive Indication of Soft Control Modes

When multiple modes exist, they should be distinctively marked so the user can determine the current mode at a glance.

Additional Information: Distinct labels may be used to indicate the currently active mode.[6635]

7.3.1-3 Coordination of Destructive and Safety-Significant Commands Across Modes

A command that produces a benign action in one mode should not cause a different action with serious negative consequences in another mode.

Additional Information: A command is an instruction provided by a user requesting a computer system to perform a particular action. Actions that are destructive (e.g., delete file) or have serious safety consequences should have unique commands. For example, the function key 'F2' should not have a benign action, such as listing a directory, in one mode but a destructive action, such as deleting a file or operating important plant equipment, in another mode.[6635]

7.3.1-4 Unique Commands for Destructive and Safety-Significant Commands

Unique commands associated with actions that have important consequences should not be easily confused with other commands used in the same or different modes.

Additional Information: Reserving special commands for special actions can prevent mode errors because, if the command is entered while the device is in the wrong mode, it will not be accepted by the system. A unique or reserved command should not be so similar to other commands that a valid entry may result from incorrectly entering another command. For example, if the command 'CNTL X' is reserved for a special action, then similar commands, such as 'ALT X' and 'Shift X,' should not be valid, even in other modes. The combination of a mode error and the incorrect entry of the command may execute an unintended action.[6635]

7.3.1-5 Discrimination of Interface Management Actions and Process Control Actions

The design of the user interface should clearly distinguish between interface management actions and process control actions.

Additional Information: Actions required for interface management tasks and plant control tasks should look different. This may be accomplished by providing different interfaces, different coding for interfaces, and, possibly, different input devices.[6635]

7.3.1-6 Reducing the Likelihood of Unintended Actuation

For actions that can have significant negative consequences, the user interface should be designed to reduce the likelihood of unintended actuation by requiring deliberate action for their execution.

Additional Information: Deliberate actions should be required for inputs having serious potential consequences. Actions that require physical effort in the form of multiple steps or higher actuation forces may be less likely to occur accidentally as the result of a random motion of the user. In addition, actions that require greater attention, such as multiple steps and checks, may reduce the likelihood that the user will revert to the type of 'automatic' activity that could cause a slip. However, control actions that require multiple steps also should be designed to reduce the likelihood of other errors (i.e., the failure to complete a set of steps in the correct order).[6635]

7.3.1-7 Feedback For Selected Actions Before Execution

The HSI should give the user feedback indicating the action that was selected and allow the action to be canceled before it is executed.

Additional Information: The goal of this recommendation is to avoid unintended manipulation of plant equipment or unintended interface management actions. Feedback about the selected option is important because a broad range of actions may be accessed through a soft control device, including manipulation of various plant components and of the user interface. The close proximity and similarity of input options within the display area may result in users selecting the wrong ones. Users should be able to cancel or modify an action if they determine that its execution would be undesirable.[6635]

7.3.1-8 Use of Error-Mitigation Approaches

Error-mitigation approaches should not be the sole means for achieving error tolerance, but should be used in conjunction with other means for error prevention and system-assisted error detection.

Additional Information: Error-mitigation mechanisms limit the effects of incorrect inputs after they have been entered into the control system. Two strategies include reducing the rate of the system's response and deferring it. Both are intended to provide time for detecting and correcting input errors and for reversing them. Error mitigation should not be considered a substitute for error prevention and detection.[6635]

7.3.1-9 Undo Features

If undo features are provided they should be consistently available.

Additional Information: Undo features minimize the effects of users' errors by allowing them to undo or reverse previous actions. Users tend to rely upon undo features and incorporate them into their work. Failures of undo features may have worse consequences than if they were not provided in the first place. For example, operators may be more willing to delete files if they think they can recover them.[6635]

7.3.2-1 Indicating the Status of Sequential Actions

Computer-based HSIs should support users in rapidly assessing the status of sequential actions in progress.

Additional Information: An action sequence is a set of operations that must be performed in a specific order. Errors involving misordering the components of an action sequence include skipped, reversed, and repeated steps. Soft controls may be more prone to this type of slip than conventional controls because they introduce additional operations for accessing controls and displays and providing inputs that also often have sequential constraints on their execution. In addition, many control operations must be performed in particular sequences. For example, when configuring a fluid system, it may be necessary to establish the flow path, control mode, and setpoint of a flow controller in a specific sequence of operations (e.g., A, B, C, D, and E). One form of error occurs when a user skips a step thinking that it was completed. For example, a user may perform operations A, B, and C and after some delay or interruption, may perform operation E thinking that D already was finished. The repetitiveness of the task is a factor in this type of error. If a user has performed a set of operations repeatedly on several identical controllers, the memory of performing a particular operation on the other controllers may increase the likelihood of the user incorrectly concluding that the operation was completed on the present controller. Thus, the sequentiality of soft controls can interact with repetitive, sequential tasks to increase the probability of errors involving misordering the components of the action sequence. The display design of computer-based HSIs should support users in identifying tasks that are in progress; ideally, they should be designed so that the status of related operations (e.g., A, B, C, D, and E) can be checked at a glance from a single display.[6635]

7.3.2-2 Drawing Attention to Points Where Similar Sequences Diverge

The design of the HSI should draw the user's attention to points where operational sequences that have multiple steps in common begin to diverge from each other.

Additional Information: A capture error occurs when an infrequently performed action requires a sequence of operations that overlaps with the sequence required for a frequently performed action. In attempting the infrequent action, the frequent one is performed instead. For example, a user intends to perform task 1, consisting of operations A, B, C, and D, but instead executes the more frequently performed task 2, (composed of operations A, B, C, and E). Capture errors often occur at the point of divergence of the frequently and infrequently performed sequences. HSI design efforts may be directed at that critical point to bring it to the user's attention. For example, if the control system knows the user's intention (e.g., by requiring an indication of the overall intention), it could highlight the proper path at the choice point, or initiate a warning if the wrong one is taken. Another approach is to draw the user's attention to important choice points (i.e., points where the sequence of operations differs from the sequences of similar tasks) by coding, labeling, and caution messages. Yet another way is to incorporate features drawing attention to the operational significance of alternative paths and supporting an understanding of which path has been taken.[6635]

7.3.2-3 Interruption of Transaction Sequences

The HSI should allow the user to interrupt or terminate a current transaction sequence.

Additional Information: A transaction sequence is a series of steps undertaken to accomplish a larger task. For example, the task of changing a control setpoint may involve multiple steps for selecting the variable and entering the new value. If different types of interruptions or terminations exist, then each should have a separate control option and a distinct name. Table 7.1 lists interruption and termination types.[6635]

Table 7.1 Different types of interruptions or terminations for transaction sequences

Back or Go Back	A nondestructive option that returns the display to the last previous transaction.
Cancel	An option that erases changes just made by the user and restores the current display to its previous state.
End, Exit, or Stop	An option that concludes a repetitive transaction sequence.
Pause and Continue	Options that interrupt and later resume a transaction sequence without any changes to either the data entries or the logic of the interrupted transaction.
Restart or Revert	An option that cancels entries made in a transaction sequence and returns the user to the beginning. If a restart will result in the loss of data or changes, a confirming action is required of the user.
Review	A nondestructive option that returns to the first display in a transaction sequence, permitting the user to review a sequence of entries and make necessary changes.
Suspend	An option that permits the user to preserve the current state of a transaction while leaving the system and permits resumption of the transaction later.

7.3.2-4 Interrupted Sequence Prompt

The HSI should support the user in maintaining awareness or recalling tasks that were interrupted or suspended by giving a reminder.

Additional Information: A loss-of-activation error occurs when an intended action is not carried out due to a failure of memory (i.e., the intention has partially or completely decayed from memory). One way of preventing loss of activation is to have an on-screen message reminding the user of the suspended task. If necessary, the system should prompt the user with information on how to resume it. A second approach is to provide more display screens or implement a window-based display system to keep tasks that are in progress visible, as they would be in spatially dedicated conventional control rooms.[6635]

7.3.2-5 Resumption of Interrupted Sequences

A minimum number of actions should be required to resume a control-action sequence that was temporarily suspended.

Additional Information: When a user has interrupted a sequence of operations, a minimum number of actions should be required to resume it. The user should not be required to restart the sequence from the beginning. One way of supporting the user in finding a display containing a suspended task is to have a 'previous display' feature that accesses a sequence of previous displays. A second approach is an interaction history feature that lists previously accessed displays and provides access to them. A third method is to include a 'bookmark' feature allowing users to designate displays containing tasks that are in progress. Thereafter, few actions or none should be required to resume the task.[6635]

7.3.3-1 Separate Action For Verification Steps

Verification steps should be separate from input actions.

Additional Information: Verification steps are usually steps added to the input action. For example, the user selects an option and then presses the Enter key to verify it. Verification steps reduce the likelihood of input errors by increasing the effort (i.e., the number of steps) and drawing users' attention to the input operation. However, they can lose their effectiveness if users can perform them unconsciously as part of the input action.[6635]

7.3.3-2 Confirmation of Goals

When feasible, confirmation steps should draw attention to the goal of the action, not just to the action.

Additional Information: Confirmation steps require the user to respond to a warning or advisory message. For example, the user may respond to the question, 'Are you sure you want to do this?' by pressing 'Yes' or 'No.' Like verification steps, confirmation steps attempt to reduce input errors by increasing the effort (i.e., the number of steps) and drawing users' attention to the input operation. A problem with confirmation steps is that they are often ill timed, occurring just after the user initiated the action and is still fully content with the choice. If the user requests an action but specifies the wrong object to be acted upon (e.g., the user requests a file deletion but specifies the wrong file), the system's request for confirmation is not likely to help the user detect the error. At this point, the user is apt to focus on confirming the action (e.g., deletion) rather than the object (e.g., which file). The potential benefits of confirmation steps should be weighed by comparing their effects on the user's response time (e.g., potential delays) to the potential consequences associated with the errors that are being guarded against.[6635]

7.3.4-1 Use of Interlocks, Lockouts, and Lockins

Interlocks, lockouts, and lockins should be provided to restrict personnel actions that may affect plant safety.

Additional Information: An interlock is a feature that requires user actions to proceed in a specific sequence. A lockout prevents personnel from providing input that may generate a negative effect. Statically defined lockouts may restrict inputs to a specific, predefined range or set of values. Context-sensitive lockouts may restrict input values based on the current situation. A lockin keeps an ongoing operation active by preventing personnel from terminating it prematurely. Personnel actions that may affect plant safety include control actions and manipulating stored data important to safe plant operation.[6635]

7.3.4-2 Override of Interlocks, Lockouts, and Lockins

The design of interlocks, lockouts, and lockins should not limit the users' authority unless there is a clear safety reason.

Additional Information: Error-prevention measures (e.g., interlocks, lockouts, and lockins) that cannot be overridden by the user may be detrimental to safety. Sometimes a normally undesirable tactic may be the only thing a user can do to solve a problem.[6635]

7.3.4-3 Visibility of Interlocks, Lockouts, and Lockins

Interlocks, lockouts, and lockins should be designed to indicate which actions are being blocked and what conditions activated the block.

Additional Information: A lockout blocks inputs that it considers unacceptable or not achievable. When this occurs, the user should be able to determine why an input was blocked and what inputs are acceptable, especially for context-sensitive validation in which complicated rules may be used for assessing the acceptability of an input value. An interlock should inform the user of the condition(s) that activated it and the conditions that must be satisfied to release it. Lockin features should show the user what action is being 'locked in' (i.e., the action that is being caused to operate without interruptions) and how it can be canceled.[6635]

7.3.4-4 Automatic Logging of the Activation of Interlocks, Lockouts, and Lockins

The activation of an interlock, lockout, or lockin should be automatically logged.[6635]

7.3.4-5 No Automatic Actuation of Blocked Actions

An interlock, lockout, or lockin should not initiate an action that was previously blocked merely because the status of the triggering condition has changed.

Additional Information: If operation B was blocked because condition A was not satisfied, the system should not automatically start operation B when condition A is met. Instead, a separate action should be required (e.g., the user should be required to take a specific action to allow operation B to resume).[6635]

7.3.5-1 Warning Message Content

Warning messages should draw users' attention to the goal of the action, not just to the action.
Additional Information: Actions may be described in many levels of detail. Often error messages are not effective because they are directed toward the wrong level of detail, so that the description of what is wrong may not match the user's understanding of what was done. An alternative is to allow the user to interrogate the warning. For example, the initial warning could be given at a very high level, corresponding to the system's understanding of the user's intent but then could allow the user to obtain information at lower, more detailed levels, such as describing how the action was performed and why it was inappropriate for the goal.[6635]

7.3.5-2 Automatic, Self-Correct Features for Interface Management Action

Automatic, self-correcting features should only be used for interface management actions, such as retrieving displays.
Additional Information: Automatic, self-correcting features detect and automatically correct errors that users make when providing inputs; for example, a 'Delete' command that is incorrectly entered as 'DLE' will be automatically changed to its correct form 'DEL' and then executed. These systems can interfere with user's activities if their error-detection facilities are overgeneralized (i.e., they interpret correct entries as being errors), since the system may substitute an incorrect response for the correct one provided by the user, thereby affecting plant operation and safety. Additional mental burdens may be imposed on the user to learn, remember, and anticipate the types of correct inputs that these systems will interpret as errors. Therefore, automated, self-correcting features should not be employed for plant-control actions. Instead, other approaches should be used, such as warnings and confirmation steps.[6635]

7.3.5-3 Undo Capabilities for Self-Correct Features

Automatic, self-correcting features should only be used if they include good 'Undo' capabilities, so that inappropriate changes made by the system can be reversed by the user.[6635]

7.3.5-4 Use of Inspection and Transfer Steps

Inspection and transfer steps should be considered if inputs are complex, or if incorrect inputs can seriously affect safety.
Additional Information: Inspection and transfer steps are intermediate steps included in a sequence of operations to create additional opportunities for detecting and correcting faulty inputs. Rather than entering data directly into the control system, the data may be sent to a holding file for review and approval. Thereafter, a command may be entered to transfer the data from the holding file into the active portion of the control system.[6635]

7.3.6-1 Identification of Plant Variables and Components

The HSI should support the identification of plant variables and components based on recognition rather than relying strictly upon recall.

Additional Information: The HSI should present the options available to users for selecting plant variables and components. For example, they may be shown via menus or mimic displays to facilitate recognition. Where there are multiple variables, their selection should not be based strictly upon the ability of operators to recall components' identification codes.[6635]

7.3.6-2 Simple Input Actions for Selection

The user should be able to select a component or variable from a display by using simple input actions.

Additional Information: Multi-step or complex input operations, such as transcribing identification codes, should be avoided. The demands of making a selection should be minimized so as not to compete with cognitive resources needed for assessing plant conditions and planning responses. However, in some cases, such as for controls that are very important to plant safety, more complex actions may be required to reduce the likelihood of accidental actuation.[6635]

7.3.6-3 Minimize Action-Sequence Errors for Selecting Plant Variables

If a sequence of actions is required to select a component or variable, the HSI should be designed to prevent misordered action-sequence errors.

Additional Information: When a soft control is used to manipulate multiple plant components or variables, the user may need to select one, perform the control action, and then deselect it before controlling the next. Errors involving misordering the components of an action sequence may occur. If the user fails to deselect the last component or variable (i.e., the one that was previously controlled), the control action may be performed on the wrong one. The HSI may minimize the likelihood of misordered action-sequence errors by minimizing the number of selection steps, reducing sequential constraints on selection steps, and providing feedback for identifying out-of-sequence steps.[6635]

7.3.6-4 Minimize the Number of Retrieval Steps for Controls that are Used Together

When a group of controls must be used together, their retrieval should require a minimal number of actions.

Additional Information: Excessive selection steps can prevent prompt access to controls and can cause misordered action-sequence errors. One approach to reducing the number of selection actions is to present, on the same display, controls that are used together.[6635]

7.3.7-1 No Activation When Display Is Inoperable

Users should not be able to activate a soft control if its display is not working.

Additional Information: A reported problem with touch screens is that sometimes their buttons may remain active even though the video image is not visible. Thus, a user could touch a blank screen and provide a valid input. Such problems may be avoided by requiring multiple actions, such as separate selection and activation steps, for inputs that may have serious consequences (e.g., affect the operation of plant equipment).[6635]

7.3.7-2 Automatic Reset of Multi-Variable Controls

If an input device controls more than one variable, the user should not have to reset the device to match the value of the new variable before executing a control action.

Additional Information: When switching between variables, the control should automatically display the current value of that variable and position the input device consistent with that value. The user should not be required to adjust the input device to match the current value of a new variable. For example, if variable A is currently set at a value of 100 and variable B at 10, when selecting the latter, the user should not be required to adjust the input device to the 10 position before executing a control action.[6635]

7.3.7-3 Numerical Input Values

The HSI should provide feedback to support the user in verifying the correctness of numerical values entered.

Additional Information: At a minimum, the value should be depicted as digital readout. However, additional feedback can further aid users in detecting input errors. For example, for control setpoints, reference values can convey the implications of the new value for plant operations and, thus, support the user in identifying a value that is too large or too small. Reference values include the actual value of the process variable, the current setpoint value, the normal operating limits, and the alarm limits. Graphical feedback might include a bar chart depicting the input value (i.e., the bar's length corresponds to the magnitude of the entered value). The reference values and the graphical representation may be combined.[6635]

7.3.8-1 Minimize the Use of Irreversible Actions

The design of the HSI should minimize the use of irreversible actions for handling stored data.
Additional Information: The design of HSI should seek to eliminate irreversible actions in handling stored data. The user should be able to reverse an action with an 'Undo' capability. If an action cannot be designed to be reversible, the user interface should be designed to reduce the likelihood of unintended actuation.[6635]

7.3.8-2 Deferring Execution of Operations that are Destructive to Stored Information

Whenever practical, irreversible operations that destroy stored information should be deferred and require a separate action for their execution rather than being carried out immediately.
Additional Information: Operations that are destructive to stored information include modification and deletion of files. One way of making actions reversible is to defer their execution, giving the user an opportunity to reconsider and reverse the action. An example is the command to delete a file. Many computers place the files in a storage location where, depending upon the computer, it may be deleted automatically in the future, or remain indefinitely until the user issues a separate command. This feature allows the user to easily recover the file. Such reversible delete features may be beneficial in NPPs for recovering trend information or other data important for the safe operation of the plant.[6635]

7.3.9-1 Actuation Feedback

Soft controls should provide feedback about their operating state after activation.
Additional Information: Momentary controls, which operate only during actuation (e.g., while a button is pressed) should provide feedback during operation. Continuous-operation controls, which remain operating after actuation, should provide continuous feedback.[6635]

7.3.9-2 Notification of Automatic Mode Changes

Systems that can change mode automatically should provide feedback to make the user aware of the current mode.
Additional Information: The HSI should inform the user of the current operating mode, mode-transition points, limits on actions, and circumstances in which users must assume control. This feedback should help the user assume control without unnecessary actions and without unnecessarily disrupting plant systems and processes.[6635]

7.3.9-3 Delaying System Response

Where appropriate, systems that are sensitive to incorrect inputs should be designed to limit the rate at which these inputs can affect the process.
Additional Information: Limiting the rate at which a system responds to a user's inputs can provide opportunities for the user to detect and correct erroneous material. Methods for delaying system response include programmed limits in the control software, such as maximum ramp rates, and physical limits in plant equipment, such as orifices and dampers, to limit the rate at which processes can respond to inputs. These methods may be used when the system's slower response will not degrade plant operation or safety. These methods should be used with other methods that prevent errors and detect them.[6635]

SECTION 8: COMPUTER-BASED PROCEDURE SYSTEM

8 COMPUTER-BASED PROCEDURE SYSTEM

Procedures are typically written documents (including both text and graphic formats) that present a series of decision and action steps to be performed by plant personnel (e.g., operators and technicians) in order to accomplish a goal safely and efficiently. NPPs use procedures for a wide variety of tasks from administration to testing, and plant operation. Computer-based procedure (CBP) systems were developed to assist personnel by computerizing paper-based procedures (PBPs). Their purpose is to guide operators' actions in performing their tasks in order to increase the likelihood that the goals of the tasks would be safely achieved. CBPs define decisions to be made and actions to be taken where the goals are unambiguous and the correct or desired course of action is generally known.

While the primary focus of the characterization presented below is focused on emergency operating procedures (EOPs), it is recognized that normal and abnormal operating procedures have been important contributors to many significant events and play a significant role in plant safety. Thus, the guidelines in this section may also apply to procedures used in testing, surveillance, troubleshooting, and maintenance, when they are delivered by CBP systems.

The design review of CBP systems requires two types of guidance: procedure guidance and HSI guidance. The first type addresses the human factors aspects of procedure design and is intended to ensure that procedures are technically correct and usable. There is considerable guidance on procedure design, e.g., NUREG-0899. In addition, HFE considerations related to the development of procedures are addressed by NUREG-0711, Rev.1 (Element 8, Procedures) and NUREG-0800 (Chapter 18).

The second type, HSI guidance, covers their design characteristics. CBPs use other HSI resources, e.g., information is presented on VDUs, and operators interact with the CBP information using dialogue and navigation capabilities provided by the computer system. Many of the characteristics of CBP design are addressed by human factors guidelines in the general sections of this document. The guidelines provided in this section emphasize HSI characteristics specific to implementing procedures in computerized form, such as features that help users manage concurrent procedures or monitor continuously applicable steps in an ongoing operation.

Two aspects of CBP system design and implementation are not addressed in this section. First, the CBP guidance does not address software aspects of CBPs. For a discussion of general software development, testing, and management see NRC Regulatory Guides 1.168 through 1.173; NRC, 1977 a-f. Second, procedure maintenance and configuration control are not addressed. While procedure maintenance and configuration control are equally important for CBPs and PBPs, these two procedure systems are likely to use different mechanisms. The following are aspects to be considered for CBPs: how procedures are entered into the computer system; how their quality is verified (e.g., no typos or omissions); how errors are identified, tracked and corrected; how changes are incorporated; and how configuration control (i.e., control over revisions and modification) is provided. NUREG-0899, NUREG-0711, Rev. 1, and NUREG-0800 contain general guidance for procedure maintenance and configuration control developed for PBPs.

The following characterization identifies CBP design features and functions important to personnel performance that can be used to describe a CBP system during an HFE design review.

INFORMATION DISPLAY

The display elements for CBP systems include the following: procedure identification information; procedure steps; warnings, cautions, notes, and supplementary information; lists; procedure organization; and format and screen layout. Each is briefly described below.

Procedure Identification Information

Procedures are identifiable to the operators and maintainers through the title, procedure number, revision number, and date. Procedures also contain statements of the high-level objective and its applicability, including the procedure category, e.g., emergency or abnormal. Review guidelines for procedure identification are provided in Section 8.1.1.

Procedure Steps

Steps are the basic unit of the procedure. Each step is composed of a verb and a direct object. In general, the rules of English grammar are followed and the syntax reflects concise language that is simply stated, explicit, and consistent. Decision steps provide instructions to evaluate conditions and then to choose appropriate action(s) from a predefined set. The decisions may involve conditional logic, i.e., where actions are to be performed only if a specified set of conditions exists. Action steps identify actions to be taken; i.e., instructions to perform physical (e.g., "Depress") and mental (e.g., "Verify") actions as well as describing the objective of those actions. Some procedure steps (e.g., in EOPs) have a dual nature, with an action to be accomplished in one column and a second action if the first is not successful. Some procedure steps may also require calculations.

Implementation of procedures has a temporal flow, i.e., some steps are taken when encountered, others are performed continuously (i.e., steps of continuous applicability), while others are done based on time or process criteria. Performance of a procedure step may be supported by information, such as cautions and notes, that qualifies the actions and decisions required. Review guidelines for procedure steps are provided in Section 8.1.2.

Warnings, Cautions, Notes, and Supplementary Information

Warnings alert operators to potential hazards of their actions that may result in death or injury to workers or the public. Cautions alert operators to potential hazards of their actions that may damage machinery or equipment. Notes call attention to important supplemental information that may enhance an operator's understanding and performance of the procedure.

Procedure steps may reference supplementary material that helps the operator implement the step; it can be in the form of tables, figures, lists, text, or numeric information. Guidelines for reviewing warnings, cautions, notes, and supplementary information are provided in Section 8.1.3.

Lists

As noted in Section 1, Information Display, a list is a display containing alphanumeric strings arranged in a single column by rows. Procedures frequently use list to present groups of items such as actions, conditions, components, criteria, and systems. When lists are used in CBPs, additional consideration must be given to the grouping of items, provision of checkoff capability, and operator alerts to items that may be overlooked. Review guidelines for these aspects of CBP lists are provided in Section 8.1.4. General review guidelines for list formats are presented in Section 1.2.2.

Procedure Organization

Nuclear plant procedures are not like simple checklists in which a user starts at the top and linearly proceeds step-by-step to the end. Based on plant conditions, the operator may be required to branch from one part of a procedure to another or from one procedure to another. Thus, the organization of procedures is an important consideration. Review guidelines for procedure organization are provided in Section 8.1.5.

Format and Screen Layout

PBPs generally present the basic steps in text or flowchart format. Both of these formats may be used in CBPs. However, unlike PBPs, CBPs are viewed through the limited display area of one or more VDUs. Thus, whether the procedure format is text or flowchart, the designer must still decide whether the

procedure will be presented to the operator in a continuous, scrollable display or divided into discrete display pages.

The overall screen layout for presentation of the procedure elements refers to the

- determination as to what information should be continuously presented
- manner in which individual procedure elements are presented.

For example, the procedure title and identification information may be continuously presented at the top of the CBP screen, while the steps are shown on scrollable window. Cautions may be represented in a separate window. The CBP may also display such supporting features as bookmarks, checklists, and operator comments.

Presentation formats, such as text and flowcharts, can be enhanced by the coding capabilities of computer-based displays, e.g., color, flashing, animation, and auditory cueing. Coding is generally used to increase the salience of important information. CBPs use coding for conditions such as:

- whether procedure step logic is satisfied or not
- whether information is static or dynamic with plant state
- when a caution is in effect
- when a change in the status of a continuously monitored step has occurred

CBPs can be designed to allow operators to choose the level of detail in which procedures are presented. For example, operators may select to have less detail displayed when a procedure step is satisfied. Alternatively, an operator may choose to show all of the individual evaluations that led to the conclusion that the step is satisfied. Guidelines for reviewing procedure formatting and screen layout are provided in Section 8.1.6.

General guidelines for information display are presented in Section 1.

A significant difference between PBPs and CBPs is in the type of functions offered by CBP systems for viewing and using the procedures. Procedure functions can be organized into four cognitive categories: Monitoring and Detection, Situation Assessment, Response Planning, and Response Implementation. In terms of monitoring and detection, operators must monitor process parameters referenced by procedures. Operators must also monitor their own procedure-related actions.

The degree of situation assessment needed in using procedures is high. While EOPs enable operators to act without diagnosing the disturbance, operators must assess whether EOP entry conditions exist. Within the procedure, operators assess each decision step by comparing actual values to the procedure's reference values, evaluating whether cautions are applicable, assessing whether each step is complete or not, and tracking and remembering their path through the procedure (the procedure history), steps of continuous applicability, and steps that are time- or parameter-value dependent. This can be difficult because steps must be evaluated while others are being performed. Operators must also assess the applicability of individual steps because PBPs are generic and not context sensitive (context sensitivity is the selection of procedural information based on plant state). Finally, operators must evaluate the success of the current procedure in achieving the high-level procedure goals and the procedure's termination conditions.

Procedures were originally designed to support response planning. In the case of EOPs, for example, the procedures were intended to assist operators in responding to events by setting out the steps necessary to achieve safety goals. It relieved the operator of the burden of formulating response plans in real time. Instead, the actions necessary to restore and maintain critical safety functions were analyzed in advance by the procedure developer and supplied as a set of detailed instructions. However, operators must still evaluate whether transitions to other parts of the procedure or other procedures are warranted. At rare

times, they may have to modify a procedure when the current plant conditions render the existing procedure inapplicable.

With respect to response implementation, the operator's responses involve actions on the procedures themselves, such as making the transition from one step to the next, to other parts of the procedure, or to other procedures. Responses also include controlling equipment based on procedural guidance. CBPs may support operators' interaction both with the procedures and with plant equipment.

While PBPs support response planning, they provide little active support for monitoring, situation assessment, and response. CBPs, on the other hand, may support these cognitive functions as well; the extent to which they do so is determined by the CBP design.

Table 8.A provides an overall scheme in which the level of automation of CBPs can be organized. This table illustrates the widely varying levels of automation and functional capabilities that CBPs may possess. It also can be used to catalogue the functional capabilities of a particular system.

In the rows, the general cognitive functions (as described above) are identified along with the procedure-related activities associated with each. In the columns, four levels of automation are identified: manual, advisory, shared, and automated. The meanings of these levels of automation are

- Manual – The function is performed by the operators with no assistance from the CBP.
- Advisory – The CBP gives advice only. For example, the CBP may advise the operator that Pump A should be started, but does not perform the action.
- Shared – The CBP and the operators both perform the function. For example, a CBP system could monitor a process but be unable to access all necessary information about the system (e.g., valve position) due to lack of instrumentation. When this type of information needs to be monitored, the operator obtains the information.
- Automated – The CBP performs the function automatically without direct intervention from the operator. This may or may not involve notification to the operators of the automated actions taken.

A given level of automation is not necessarily meaningful for all functions. For example, with respect to process monitoring, it is not meaningful to have an advisory level of automation. The CBP system will either have monitoring capability or it will not. This is indicated by NA (not applicable) in the table.

A given procedure system may make no provisions for a given function. For example, a CBP may not address control of equipment in any capacity, not even manual. In such a system, equipment would be operated using the other resources of the HSI. Thus, the entire function is not applicable for that specific CBP.

Individual CBP systems differ in terms of the levels of automation they provide. To achieve these varying levels of automation, CBPs may need to provide features that go beyond those identified above as the basic procedure elements. For example, to provide for manual control of plant components, the CBP would need to include a control, e.g., a soft control, for that equipment.

Review guidelines for functional capabilities of CBPs are given for the following specific topics:

- Procedure supervision and control (in Section 8.2.1)
- Procedure monitoring and assessment (in Section 8.2.2)
- Monitoring of user actions (in Section 8.2.3)
- Planning and implementation (in Section 8.2.4).

Table 8.A Levels of automation of procedure functions

Procedure Functions	Level of Automation[1]			
	Manual	Advisory	Shared	Automatic
Monitoring and Detection				
Process parameter values		NA		
Operator actions		NA		
Situation Assessment				
Procedure entry conditions		NA		
Resolution of procedure step logic		NA		
Step status (incomplete or completed)		NA		
Procedure history		NA		
Context sensitive step presentation		NA		
Assessment of continuous, time, and parameter steps		NA		
Assessment of cautions		NA		
High-level goal attainment and procedure exit conditions		NA		
Response Planning				
Selection of next step or procedure				
Procedure modification based on current situation				
Response Implementation				
Transition from one step to the next				
Transition to other parts of procedure of other procedures				
Control of plant equipment				

[1] NA means "not applicable." For a given CBP system, a level of automation may not be applicable or an entire function may not be applicable.

USER-SYSTEM INTERACTION

CBP systems have special requirements to support the operator's interaction with the system, procedure maintenance and configuration control. CBP-specific interface management considerations (such navigation aids) include the need to make transitions between procedure steps and between different procedures. In addition, procedure use can be supported by automated facilities that monitor and record the operator's actions and provide support for interface management tasks when needed. User-system interactions specifically addressed by the review guidelines include: path monitoring (see Section 8.3.1), navigation (see Section 8.3.2), and help (see Section 8.3.3). General guidelines for user-system interaction are found in Section 2.

The types of devices used to operate the CBP system should be identified, including computer-based input devices (e.g., alphanumeric keyboards, trackballs, mice, and touch screens), conventional controls, and soft controls, as described in Sections 3 and 7. Guidelines pertaining to the hardware used to implement computer-based procedures are given in Section 8.4.

BACKUP CAPABILITIES

CBPs can fail or malfunction. When important operations cannot be suspended or put off while the system is repaired, backup to the CBP is necessary. In the case of EOPs, a delay in operations in the event of a failure is not acceptable, therefore, some form of procedure backup is warranted. Review guidelines for procedure backups systems are provided in Section 8.5.

INTEGRATION WITH OTHER HSI ELEMENTS

The integration of the CBP with other resources of the HSI must be considered. Depending on the level of automation, as shown in Table 8.A, CBP systems will require varying types of interfacing with the remainder of the HSI. The consistency and compatibility of the CBP with the rest of the HSI can affect operator performance. Thus, important considerations in the CBP review include the degree to which (1) the display of plant variables in the CBP is compatible with the normal monitoring displays, (2) compatible coding schemes are used, and (3) control implementation modes of the CBP are consistent with the rest of the HSI (e.g., with modes of automated control systems). Guidelines for reviewing the integration of CBP with other HSI components are provided in Section 8.6.

In the course of developing the guidance for CBPs, several considerations were identified that are important to crew performance and safety, but for which the technical basis was insufficient to develop specific HFE guidelines. These aspects of computer-based procedure design should be addressed on a case-by-case basis using the design process considerations presented in Appendix B3.

8 COMPUTER-BASED PROCEDURE SYSTEM
8.1 Information Display
8.1.1 Procedure Identification

8.1.1-1 Procedure Title and Identification Information
Each procedure should contain identifying information including title, procedure number, revision number, date, and organizational approval.
Additional Information: This information helps the user establish the appropriate context for using the procedure.[6634]

8.1.1-2 High-Level Goals
Each procedure should state its high-level goals and applicability, including its procedure category, e.g., emergency or abnormal.
Additional Information: Information should be given allowing the user to understand the purpose or goal of a series of steps and supporting the user's assessment of the success of the procedure in achieving its safety goal.[6634]

8.1.2-1 Concise Steps
Procedure steps should be concise.
Additional Information: Steps should be designed to communicate information clearly and unambiguously so that they can be easily understood and interpreted without error.[6634]

8.1.2-2 Short Sentences
Procedure steps should be written as short sentences.[6634]

8.1.2-3 Active Voice
Procedure steps should be written in active voice.[6634]

8.1.2-4 Positive Commands
Procedure steps should be written as positive commands.[6634]

8.1.2-5 Simple Wording
Short, simple words from standard American English should be used.[6634]

8.1.2-6 Standard Punctuation
Punctuation should conform to standard American English usage.[6634]

8.1.2-7 Consistent Word References
Words, phrases, and equipment names and numbers should be used consistently within and among procedures, drawings, other HSIs, and equipment labels.[6634]

8.1.2-8 Abbreviations and Acronyms
Abbreviations and acronyms should be used consistently and limited to those well known to the users.[6634]

8.1.2-9 Units of Measures
Numerical information should include units of measure.[6634]

8.1.2-10 Numerical Precision
Numbers should be specified at the appropriate precision.[6634]

8.1.2-11 Number Ranges
Ranges of numbers should be specified, rather than error bands.[6634]

8.1.2-12 Use Arabic Numerals
Arabic numerals should be used.[6634]

8.1.2-13 Spelled Numbers
Numbers that are spelled out should be consistently spelled under the same conditions.[6634]

8.1.2-14 Presentation of Conditional Steps
Conditional steps should be shown in traditional text formats following the guidance in Appendix B of NUREG-0899.[6634]

8.1.2-15 Specification of Preconditions for Steps
The procedure should specify any conditions that must be met before an action can be undertaken.

8 COMPUTER-BASED PROCEDURE SYSTEM
8.1 Information Display
8.1.2 Basic Steps

Additional Information: Information about preconditions in the procedure should be located so that users read the information before acting. Information given in other locations may be overlooked, or require additional actions to retrieve it, which may be distracting and time consuming. Further, if conditions are implied, users may easily miss or misinterpret them.[6634]

8.1.3-1 Parallel Display with Procedure Step

The warnings and cautions applicable to a single step (or to a series of steps) should be displayed when the step(s) is on the screen.

Additional Information: Displaying warnings and cautions at the same time as their associated procedure steps will help ensure that users read the information when they evaluate the step. Information provided elsewhere may be overlooked, or may require retrieval by distracting and time-consuming actions.[6634]

8.1.3-2 Position Before Action Steps

Warnings, cautions, and notes should be presented so that they will be read before the applicable action steps.

Additional Information: Displaying warnings, cautions, and notes before action steps will help ensure that users will read the information before taking action. Information provided in other places may be overlooked or may be distracting and time consuming to retrieve.[6634]

8.1.3-3 Action References

Warnings, cautions, and notes should not include implied or actual action steps.

Additional Information: Actions should be specified in procedure steps only.[6634]

8.1.3-4 Distinction from Other Procedure Elements

Warnings, cautions, and notes should be uniquely presented, so that they are easily distinguished from each other and from other display elements.[6634]

8.1.3-5 Supplementary Information

All supplementary information (such as tables and figures) required for a procedure step and available to the CBP should be shown on the screen concurrently with the step, or on another easily viewed display.[6634]

8.1.4-1 Appropriate Application of Lists

Groups of three or more related items (e.g., actions, conditions, components, criteria, systems) should be presented as a list.[6634]

8.1.4-2 Distinction from Other Procedure Elements

Formatting should be used to differentiate items in a list from other procedure elements.[6634]

8.1.4-3 Identification of Precedence

The presence or absence of precedence among items in lists should be indicated.
Additional Information: It should be clear to users whether some items take precedence over others.[6634]

8.1.4-4 List Overviews

Overviews should introduce each list.
Additional Information: An example of an overview is "Ensure that all of the following tests were completed:".[6634]

8.1.4-5 Assuring Users' Attention

The method for assuring that each item in a list has received the users' attention should be consistent.
Additional Information: For example, an electronic checklist may be provided so that users can check off items they have attended to. If users proceed before all items are checked off, the CBP may alert them to the unchecked items.[6634]

8 COMPUTER-BASED PROCEDURE SYSTEM
8.1 Information Display
8.1.5 Organization of Procedures

8.1.5-1 Hierarchical, Logical Organization
The procedures should be organized in a hierarchical, logical, consistent manner.
Additional Information: Organization will make it easier for users to see the relationships among procedures.[6634]

8.1.5-2 Organization of Procedure Steps
Each procedure should be organized into sections of related steps.[6634]

8.1.6-1 Organization Format of Procedures

The procedure's format should reflect its organization.
Additional Information: Formatting methods to indicate the organization of a procedure may include the use of headings or colors to distinguish parts of the procedure.[6634]

8.1.6-2 Format of Procedures

A consistent format should be used to display procedures.
Additional Information: Whether procedures are presented in text, flowchart, or otherwise, a consistent approach across procedures will facilitate using and moving between multiple procedures.[6634]

8.1.6-3 Partitioning Procedures

A consistent approach to partitioning procedures should be used.
Additional Information: Partitioning refers to how a procedure is organized to be displayed on the VDU screen. For example, it may be divided into distinct pages, and users would navigate from one to the next. Alternatively, it may be presented as one continuous display that the user scrolls.[6634]

8.1.6-4 Organization of Display Screen

Each display screen should locate information and HSI features consistently.
Additional Information: When the information and features, such as procedure steps, controls, and navigation aids are consistently located, users' performance improves because expectations can guide the search for information, and reduce the time and workload associated with finding it.[6634]

8.1.6-5 Continuously Presented Procedure Information

The procedure's title and identification should be continuously presented.
Additional Information: This information helps set the context for the overall procedure within which its steps are interpreted. It is especially important when more than one procedure can be open at one time.[6634]

8.1.6-6 Continuously Presented Status of High-Level Goals

The status of high-level procedure goals should be continuously presented.
Additional Information: This information helps set the overall context in which procedure steps are interpreted. Continuous presentation of high-level goal status, such as status of critical safety functions, will facilitate users' awareness of them, particularly when more than one procedure is open simultaneously.[6634]

8.2.1-1 Users' Control of Procedure Path
Users should be in control of the sequence of steps that are followed.
Additional Information: Most procedures have specifically defined steps that have to be performed sequentially, and others that can be varied at the user's discretion; CBPs should identify which one is applicable. However, users should have the flexibility to move around within the procedure, so that they can check and make verifications.[6634]

8.2.1-2 Users' Control of Pace of Procedures
Users should be in control of the pace at which procedure steps are followed.
Additional Information: Users need to maintain situation awareness of procedure-related decisions. To accomplish this, they must be in control of the pace at which steps are followed.[6634]

8.2.1-3 Understandability of Analysis of Procedure Steps
The methods by which CBPs analyze procedure steps should be consistent with the methods by which users analyze steps in procedure logic steps, so that the results are understandable.
Additional Information: Users must be able to judge the acceptability of the CBP's advice and recommendations.[6634]

8.2.1-4 Users' Verification of CBP Information
The users should be able to verify the system's assessment of plant status.
Additional Information: This verification includes process parameters, equipment status, analysis of procedure step logic, and evaluation of cautions. Any analysis done by the CBP should be accessible to users for review.[6634]

8.2.1-5 Users' Override of CBP
Users should be able to override any CBP information, calculation, evaluation, or assessment.[6634]

8.2.2-1 Automatic Identification of Procedures

The CBP should alert users when entry conditions to a procedure are satisfied.
Additional Information: This capability will help users determine the appropriate procedures for the existing plant situation.[6634]

8.2.2-2 Automatic Monitoring of Plant Parameters and Equipment Status

The CBP should automatically provide accurate and valid information on the values of parameters and status of equipment, when they are available to the system.
Additional Information: It should be clear to users what specific information is used as the source of these actual values and states.[6634]

8.2.2-3 Frequent Monitoring

The CBP should frequently monitor procedure-defined parameters.
Additional Information: Frequent monitoring, such as twice a second, promptly notifies users of status changes.[6634]

8.2.2-4 Automatic Calculation of Procedure-Referenced Values

The system should undertake calculations, such as subcooling margin, that are required when using procedures.[6634]

8.2.2-5 Analysis of Step Logic

The CBP should evaluate the logic of each procedure step and show the results to the user.
Additional Information: Procedure steps often contain logical relationships; for example, actions are to be performed if an identified set of conditions exists. The analysis of these logical relationships must be carefully verified to avoid underspecification. This occurs when the logic used to resolve a procedure step is too simplified, and does not address all of the considerations that users do when evaluating the step.[6634]

8.2.2-6 Continuous Analysis of Non-Current Step Logic

Steps of continuous applicability, time-dependent steps, and process-dependent steps should be monitored by the CBP and the user should be alerted when conditions in those steps become effective.
Additional Information: The analysis must be carefully verified to avoid underspecifying its logic. The alert should not automatically remove the user's current display. Instead, it should be presented as a supplemental display or as an alert.[6634]

8.2.2-7 Coding of Logical Analysis

When procedure's step logic indicates a violation of the step, the information should be coded to make that step more salient to users.[6634]

8.2.2-8 Analysis of Cautions

The conditions described in cautions should be automatically monitored by the CBP system, and the user should be alerted when the caution is in effect.
Additional Information: Evaluating cautions and alerting users to their applicability will ensure that users will read the information at the appropriate time, and reduce the chance that it may be overlooked. The conditions for cautions must be established with care such that the logic is not underspecified.[6634]

8.2.2-9 Coding Applicable Cautions

CBPs should use coding to indicate when a caution is in effect.

Additional Information: Coding techniques, such as color coding, may be used to enhance the salience of important information.[6634]

8.2.2-10 Users' Acknowledgment of Procedure Analyses
Users should make some form of acknowledgment of procedure steps and recommendations for terminations and transitions.
Additional Information: As an example, users may acknowledge that a step is satisfied by depressing the "Return" key, or clicking on an onscreen acceptance button. Such acknowledgment helps the users to maintain awareness of the procedure's status.[6634]

8.2.2-11 Identification of User Input Requirements
The CBP should provide users with clear, timely indications when they need to input any information not available to it.
Additional Information: CBPs may rely on users to process parameter values, equipment status (such as whether a valve is open or closed), analyses of logic steps where users' judgment is involved, or to assess any conditions not within the capability of the CBP.[6634]

8.2.2-12 Adjustable Level of Detail
Users should be able to choose the level of detail with which procedures are presented.
Additional Information: While plant practices on using procedures may be specified by management, there may be flexibility in the level of detail that can be provided. For example, users may want less detail when a procedure step is satisfied. Alternatively, a user may choose to see all of the individual evaluations leading to the conclusion that the step was satisfied. This must be done with care so that it does not affect the interpretation of procedure information. In addition, users should be trained as to how and when to vary levels of detail.[6634]

8.2.2-13 Context-Specific Guidance
Procedure guidance should be context sensitive where possible.
Additional Information: For example, the CBP system should not indicate an action to start a pump when it can determine that the pump is already running.[6634]

8.2.2-14 Assessment of High-Level Goal Status
The CBP should continuously assess and present the status of higher-level safety goals, such as critical safety functions, and alert the user to any challenges.[6634]

8.2.2-15 Assessment of Conditions Terminating a Procedure
The CBP should automatically identify when conditions are met for transitioning or exiting from a procedure.
Additional Information: This capability will help users determine when procedures they are using are no longer appropriate for the existing situation.[6634]

8.2.3-1 Monitoring Users

User responses to procedures should be monitored and recorded by the CBP.

Additional Information: Monitoring information on users' input to information requested by the procedure and their subsequent actions is necessary if the CBP is to properly assess appropriate procedural pathways.[6634]

8.2.3-2 Alert Users to Deviations in Procedure

Users should be alerted if their input is incorrect, or when their actions are not consistent with CBP evaluations.

Additional Information: The alert should be advisory and not discourage the user's actions. This feature must be supported with training, so users are not reluctant to go against the CBP's evaluations.[6634]

8.2.4-1 Display of Action Status

The status of procedure-related actions should be displayed by the CBP.[6634]

8.2.4-2 Timing of Procedures

The CBP's timing, such as status update rates, screen changes, and navigation features, should be consistent with the time demands of the task.[6634]

8.3.1-1 Monitoring Step Status

There should be an indication of whether or not a step was completed.
Additional Information: The indication can be manual or automatic, depending on whether the CBP has the specific criteria and information to determine this.[6634]

8.3.1-2 Alert User to Incomplete Procedure Steps

Users should be alerted to incomplete procedure steps.
Additional Information: The alert should be advisory and not discourage the crew's actions.[6634]

8.3.1-3 Coding Current Location

The current procedure step(s) should be indicated.[6634]

8.3.1-4 Automatic Path Monitoring

The pathway taken through procedures should be stored and made available to users.
Additional Information: A history should be maintained and available for display on request. Step completion can be time stamped to facilitate post-hoc incident analysis.[6634]

8.3.1-5 Indication of Multiple Active Procedures

The user should be informed when multiple procedures or multiple procedure steps are to be followed concurrently. A list of all currently active procedures should be available.
Additional Information: It may be helpful for the list of active procedures to include start and stop times for the procedures in use.[6634]

8.3.2-1 Flexible Navigation

Navigation support should allow users to freely and easily move between procedure steps, to other parts of the same procedure, and to other procedures.

Additional Information: Users should not be forced to access procedures in a fixed sequence of the procedure nor should their access to supporting information be limited. (See also the additional information for Guideline 8.2.1-1.)[6634]

8.3.2-2 Support Parallel Access to Information

The CBP should have the ability to access more than one piece of information at once.[6634]

8.3.2-3 Navigational Links to Related Information

Navigational links to cross-referenced information and to notes, cautions, warnings, reference material, and communication and help facilities should be provided.

Additional Information: Techniques such as hyperlinks can expedite navigation to information material cross-referenced in a procedure or its supporting material.[6634]

8.3.2-4 Access to Contingency Actions

Users should be able to easily access appropriate contingency actions.[6634]

8.3.3-1 Explanation Facilities

CBPs should have facilities to enable the user to determine how CBP functions are performed.
Additional Information: When CBPs support users' decision making, such as offering advice on how to select procedures, analyze step logic or follow procedure paths, users should be able to query the basis for the advice. Cooperative dialogue enables the user to better understand and utilize the system.[6634]

8.3.3-2 Help Facilities

Help for performing procedure specified activities should be provided.[6634]

8.3.3-3 Note Taking

There should be a way for users to record their notes and comments in the CBP.[6634]

8.4-1 Number of VDUs

The number of VDUs on which CBP information is displayed should be sufficient to provide all the procedure-related information needed for a procedure step, including cautions and reference material.[6634]

8.5-1 Paper-Based Procedure Availability

PBPs should be available in the event of CBP failure.[6634]

8.5-2 Consistency of PBPs and CBPs

The content and presentation of procedure information in PBPs and CBPs should be consistent.
Additional Information: Smooth transfer between CBPs and PBPs and vice versa will be facilitated by the degree to which their formatting is consistent; this also will facilitate training in procedure use.[6634]

8.5-3 Support for Transfer to PBPs

Upon transfer to PBPs, a means should be provided to support the user's determination of currently open procedures, location in the procedures, completed and not completed steps, and currently monitored steps.
Additional Information: When the CBP is lost, it may be difficult for users to reconstruct this information from memory. Therefore, the user should be supported in making a safe, easy transition. For example, a CBP system might automatically print out a status sheet with this information once every minute so that if it fails, the user can retrieve the latest sheet and use it to establish the crew's tasks for using PBPs.[6634]

8.6-1 Consistency with HSI

The detailed CBP design should be fully consistent with the rest of the HSI.

Additional Information: HSI features for format and functionality (such as labeling, acronyms, dialog conventions, use of colors, and input devices) should be consistent between the CBP and other HSI components. Consistency may be a special consideration when reviewing 'off-the-shelf' systems.[6634]

SECTION 9: COMPUTERIZED OPERATOR SUPPORT SYSTEM

9 COMPUTERIZED OPERATOR SUPPORT SYSTEM

Computerized operator support systems (COSSs) use computer technology to support operators in cognitive activities such as situation assessment and response planning. Based on their analyses, COSSs may provide recommendations or warnings to personnel. Example applications include: fault detection and diagnosis, safety function monitoring, plant performance monitoring, core monitoring, maintenance advising, and operator support for plant control. While the particular focus of the guidelines is on systems that support operator performance, it is also relevant to aids for others, such as maintenance personnel.

Only general guidelines for COSSs are available, and they are given in Section 9.1. Aspects of COSSs addressed in that section include alerts provided to the user regarding the availability of critical information or to notify the user that a user when a problem or situation is beyond the capabilities of the COSS; strategic planning capabilities (i.e., for evaluating the user's plans); user input to problem solving capabilities; capabilities for explaining rules, knowledge bases, problem solutions and for indicating the certainty in the correctness of analyses; and capabilities for recalling previously evoked rules and the corresponding events.

9 COMPUTERIZED OPERATOR SUPPORT SYSTEM
9.1 General

9.1-1 Consistency with User Task Requirements
The support provided by the COSS should be consistent in content and format with the cognitive strategies and mental models employed by the user.
Additional Information: Users should be able to understand the analysis logic employed by the COSS. This supports user acceptance and enables users to supervise the COSS in order to properly evaluate and utilize its output.[5908]

9.1-2 Consistency with General HSI
The COSS should be fully integrated with and consistent with the rest of the HSI.
Additional Information: The COSS's depiction of the system should utilize the same nomenclature, abbreviations, acronyms, symbology, iconic representations, and coding techniques as the general information display system.[5908]

9.1-3 Interaction With Ongoing Tasks
Use of the COSS should not require canceling ongoing tasks.[5908]

9.1-4 Critical Information Alert
If critical information becomes available during COSS utilization, the system should alert the user to the critical information.[5908]

9.1-5 Minimize Querying of User
COSS querying of the user for information should be minimized.[5908]

9.1-6 Dialogue Sequencing Flexibility
The user-COSS dialogue should be flexible in terms of the type and sequencing of user input the COSS will accept.[5908]

9.1-7 Strategy Planning Capability
The COSS should provide the capability to plan a strategy for addressing a problem.
Additional Information: The capability provided by the COSS should include: planning aids (such as time lines and worksheets); an evaluation function which assesses the adequacy of the user's plan and recommends revisions where necessary; the ability to form, state, and test hypotheses in a manner consistent with the user's plan; and the capacity to store and recall plans.[5908]

9.1-8 User Supported Strategy Selection
When the COSS is capable of a range of problem-solving strategies, it should be capable of accepting direction from the user in terms of which strategy to employ.[5908]

9.1-9 Simulation Mode Command and Identification
If the COSS has a simulation mode, entering the simulation mode should require an explicit command and result in a distinguishable change in system output.
Additional Information: A blinking "Simulation Mode" symbol, for example, can be used to clearly distinguish simulation from other operational modes.[5908]

9.1-10 Explanation Capability
The COSS should be capable of interactively explaining its rules, knowledge base, and problem solutions at any point during a user-COSS transaction.

Additional Information: Rules should be represented explicitly in the knowledge base and encoded such that they are accessible to the explanation facility and can be translated for human understanding. The COSS should respond to user requests to clarify questions and assertions. At the request of the user, the system should be capable of displaying rule-based and descriptive explanations.[5908]

9.1-11 User Control of Explanation Detail

The level of detail of information presented as part of an explanation or justification should be under the control of the user.[5908]

9.1-12 Indication of Certainty

The COSS should represent its certainty in the correctness of analyses and provide the rationale underlying the certainty estimation.
Additional Information: Certainty factors, for example, can be represented as a decimal number from -1 to +1, with -1 indicating absolute certainty that a fact is not true, and +1 indicating absolute certainty that a fact is true.[5908]

9.1-13 Inadequate Knowledge Alert

The COSS should alert the user when a problem or situation is beyond its capabilities.
Additional Information: Rule exceptions should be explicitly contained in the knowledge base and available to the user as part of the explanation facility. Where possible, the COSS should inform the user as to what additional knowledge or rules are required to complete the transaction.[5908]

9.1-14 Graphic Representation of Rules

The COSS should be able to graphically represent system relationships, its rules network, and reasoning process.[5908]

9.1-15 Highlight of Status Changes After COSS Utilization

At the completion of a user-COSS session, the COSS should update and highlight changes in the status of important system information.
Additional Information: User acknowledgement may be requested for important changes.[5908]

9.1-16 Post Hoc Rule-Event Recall

The COSS explanation facility should have the capability to recall each invoked rule and associate it with a specific event (i.e., question or conclusion) to explain the rationale for the event.
Additional Information: The COSS should automatically record all rules invoked during an analysis.[5908]

9.1-17 Rapid Interaction Retrieval

The system should permit rapid retrieval of previous exchanges between the user and the COSS.[5908]

9.1-18 Hardcopy of COSS Utilization

The user should be capable of requesting a hardcopy of data including screen displays (text or graphics), data employed during a consultation, summaries of consultations, lists of rules/facts invoked during a consultation, and summaries of hypotheses tested.[5908]

SECTION 10: COMMUNICATION SYSTEM

10 COMMUNICATION SYSTEM

COMMUNICATION SYSTEM FUNCTIONS

Crew communication is essential to performance, including communication between personnel in the main control room, between the main control room and local sites within the plant, and across sites within the plant. The communication system supports these activities. The broad variety of communication media that may be employed can be generally categorized as speech-based and computer-based communications, as described below.

SPEECH-BASED COMMUNICATION

Within the main control room, personnel generally communicate directly via unaided speech. An exception may be when personnel are separated by a large distance, such as when an operator at a main control panel must communicate with another operator located at a back panel or an auxiliary area in the control room. In such cases, a communication device may be used. In addition, communication devices are often used to communicate between the main control room and local sites within the plant, and across sites within the plant. General review guidelines for speech-based communication systems are provided in Section 10.2.1. Varieties of communication devices that may be used to support speech-based communication are described below.

Conventional telephone systems

Earphones and microphones may have variety of configurations including handsets, headsets, and surface-mounted (i.e., as in a speaker phone configuration). Headsets may cover one ear (monaural) or two (binaural). A telephone system may interface with an announcing (public address) system. Review guidelines for conventional-powered telephone systems are provided in Section 10.2.2.

Sound-powered telephone systems

Sound-powered telephone systems do not require a separate electrical power supply to transmit signals; the force of the user's speech upon the mouthpiece generates small electrical impulses, which are transmitted as a signal. Therefore, they may be beneficial for situations in which electricity is not available. Sound-powered telephones are connected to transmission wires and may be made portable by providing jacks at locations where the phone is to be used. If a sound-powered telephone system has multiple connections, it may be implemented as a "party line" unless a switching function is implemented. The switching function may be manual, unless supplemental power is provided for this function. Sound-powered telephones are often implemented with headsets. Sound-powered telephone systems require supplemental electrical power (e.g., a hand-operated crank) to energize a ringing function. In addition, the sound-powered transmitter may have an interface with a paging system so that the desired party can be called to the line. Review guidelines for sound-powered telephone systems are provided in Section 10.2.3.

Portable radio transceivers

Portable radio transceivers include battery-powered communication devices that transmit messages through the airways rather than through wires. Review guidelines are provided in Section 10.2.4.

Announcing (public address) systems

These systems generally feature loudspeakers installed in predetermined locations. In some installations, microphone input may be provided through a telephone system connection. This allows users to access the announcing system from multiple locations. Some announcing systems provide two-way

communication (e.g., via distributed microphones) allowing them to function as point-to-point intercom systems in addition to being public address systems. Review guidelines are provided in Section 10.2.5.

Fixed-base UHF transceivers

Like portable radio transceivers, fixed-base UHF transceivers transmit messages through the airways. Fixed-base UHF transceivers are not portable but may have greater frequency response than portable radio transceivers. Review guidelines are provided in Section 10.2.6.

Point-to-point intercom systems

These systems provide two-way communications via a distributed set of microphones and speakers. Review guidelines for this topic are also found in Section 10.2.6.

Emergency Communications

Emergency (i.e., backup) communications systems support internal and external communications during abnormal conditions. Review guidelines for emergency communication systems are provided in Section 10.2.7.

COMPUTER-BASED COMMUNICATION

Because of continued advances in computer-based technologies, many types of computer-based communications systems are possible; general guidelines for such systems are given in Section 10.3.1. The systems use computers to support personnel in preparing, sending, and receiving messages; specific guidelines related to these functions are given in Section 10.3.2, 10.3.3, and 10.3.4, respectively. Computer-based communication systems may allow messages to be prepared, stored, and received in a variety of formats. For example, voice mail systems handle messages primarily in verbal format, while electronic mail may handle messages in text, graphic, and auditory forms. In addition, computer-based communication systems can initiate messages automatically, such as by sending a text or verbal message to a recipient when a particular condition occurs.

Computer-based communication systems also have the following are characteristics:

- Purpose – The purpose provides a basis for identifying and assessing the relevance and appropriateness of the functional capabilities and design features of a computer-based communication system. Some considerations to be addressed include the intended users of the system, the types of communication, the locations to be covered, and the conditions under which the system is to be used (e.g., normal operations versus emergencies).
- Functional Capabilities – Functional capabilities refers to the functions performed by the computer-based communication system. Specific considerations include: support for message preparation (e.g., data entry, formatting), message sending (e.g., address directories, message priority, reply capabilities), and message receipt (e.g., message filtering and selection; time stamps; storage and retrieval; methods of receipt such as via file, display, and printer; and annotation of received messages).
- Information Display – Information display, as described in Section 1, refers to the way that information is organized and presented to the user in terms of display elements, formats, and networks. It also includes the data quality and update characteristics and characteristics of the display devices. For an HFE design review, these characteristics should be identified for the computer-based communication system. General guidelines for information display are presented Section 1.
- User-System Interaction – User-system interaction refers to the types of interaction provided between the user and the computer-based communication system. It includes input formats, cursor

characteristics, system response, the management of displays, the management of information, error response, and system security. General guidelines for user-system interaction are found in Section 2.

- Controls – The types of devices used to interact with the computer-based communication system should be identified, including computer-based input devices, conventional controls, and soft controls. General guidelines for computer-based input devices and conventional controls are found in Section 3. General guidelines for soft controls are found in Section 7.
- Backup Capabilities – If the failure or loss of availability of the computer-based communication system may affect operator tasks that are important to plant safety, then backup systems and capabilities should be included in the characterization.
- Integration with Other HSI Components – The consistency and compatibility of the computer-based communication system with the rest of the HSI can affect operator performance. Thus, important review considerations include the degree to which controls and displays of the computer-based communication system are compatible with other controls and displays of the HSI. This extends to such considerations as display formats, coding schemes, and methods of operation.

10 COMMUNICATION SYSTEM

10.1 General Communication Guidelines

10.1-1 Accessibility

Communications functions and/or equipment should be accessible from the user's normal working location.

Additional Information: Where communication requirements necessitate the use of several handsets, the accessibility of their standby locations should be determined by operational priority, i.e., the most frequently or urgently needed handset should be the most accessible. The handsets may also be color coded.[5908]

10.1-2 Instructions

Instructions should be provided for use of each communication system, including suggested alternatives if a system becomes inoperable.[0700]

10.1-3 Outgoing Emergency Messages

Priority procedures should be established for the transmission of emergency messages from the control room by any of the communication systems.[0700]

10.1-4 Incoming Emergency Messages

Procedures should be established for handling communications during an emergency, and these procedures must be known by all users.[0700]

10.1-5 Minimal User Actions

Communication systems should be designed to minimize required user actions.

Additional Information: In some applications, for example, software logic might prepare and transmit messages automatically, derived from data already stored in the computer; software logic might provide automatic reformatting of stored data for transmission, where format change is required; and interface software might provide automatic insertion into messages of standard header information, and distribution lists.[5908]

10.1-6 Communication Flexibility

Users should have flexibility in communications methods.

Additional Information: Where communications are critical, users should not be precluded from communicating with other plant personnel by the loss of one method.[5908]

10.2.1-1 Comfort

Communication equipment to be worn should be designed to preclude discomfort.
Additional Information: Supporting structures for earpieces should not impose discomforts of weight, concentrated pressures, or metal contact with the skin.[5908, 0700]

10.2.1-2 Hands-Free Operation

Communication equipment should be designed to permit hands-free operation.
Additional Information: Hands-free operation may have to be compromised to accommodate a push-to-talk switch in anticipation of possible use in areas of high ambient noise.[5908, 0700]

10.2.1-3 Frequency Response

Microphones and associated amplification equipment should be designed to respond optimally to that part of the speech spectrum most essential to speech intelligibility (i.e., 200 to 6,100 Hz).
Additional Information: Where system engineering necessitates speech-transmission dynamic range bandwidths narrower than 200 to 6,100 Hz, the minimum acceptable frequency range is 250 to 4,000 Hz. The system should achieve at least standard telephone sound quality.[5908, 0700]

10.2.1-4 Microphone Dynamic Range

The dynamic range of a microphone used with a selected amplifier should be great enough to admit variations in signal input of at least 50 dB.[5908]

10.2.1-5 Microphone Noise Shields

When ambient noise is high (85 dB(A) or greater), the microphone should be put in a noise shield.
Additional Information: Noise shields should be designed to meet the following requirements:

- Volume of at least 15.25 cubic inches (250 cubic centimeters) to permit a pressure gradient microphone to function normally
- A good seal against the face with the pressure of the hand or tension of straps
- A hole or combination of holes covering a total area of 0.1 in (65 mm) in the shield to prevent pressure buildup
- Prevention of a standing wave pattern by shape or by use of sound absorbing material
- No impediment to voice effort, mouth or jaw movement, or breathing [5908]

10.2.1-6 Noise-Canceling Microphones

In very loud, low frequency noise environments (100 dB overall), noise-canceling microphones should be used.
Additional Information: The noise-canceling microphones should be capable of effecting an improvement of not less than 10 dB peak speech-to-root-mean-square-noise ratio, as compared with non-noise-canceling microphones of equivalent transmission characteristics.[5908]

10.2.1-7 Signal Processing

If the environment or the speech transmission equipment is such that the signal-to-noise ratio of the speech is degraded, signal-processing techniques should be used to maintain speech intelligibility.

Additional Information: Where speech signals are to be transmitted over channels showing less than 15 dB peak speech-to-root-mean-square-noise ratios, peak clipping of 12 to 20 dB may be employed at system input. If necessary, clipping may be preceded by frequency pre-emphasis. The frequency pre-emphasis should have a positive slope frequency characteristic no greater than 18 dB per octave from 140 to 1,500 Hz, and no greater than 9 dB per octave over the frequency range 1,500 to 4,800 Hz, when no clipping is used. When transmission equipment employs pre-emphasis and peak clipping is not used, reception equipment should employ frequency de-emphasis of characteristics complementary to those of pre-emphasis only if it improves intelligibility. Frequency de-emphasis should be a negative-slope frequency response not greater than 9 dB per octave over the frequency range 140 to 4,800 Hz.[5908]

10.2.1-8 Speaker Frequency Range

Loudspeakers, earpieces, and headphone elements should respond uniformly (plus or minus 5 dB) over the range 100 to 4,800 Hz.

Additional Information: Headphones and loudspeakers are subject to the same frequency response restrictions as microphones and transmission equipment.[5908]

10.2.1-9 Binaural Headsets For High Noise Environments

If listeners will be working in high ambient noise (85 dB(A) or above), binaural headsets should be provided rather than monaural headsets.

Additional Information: Unless operational requirements dictate otherwise, binaural headsets should be wired so that the sound reaches the two ears in opposing phases. Their attenuation qualities should be capable of reducing the ambient noise level to less than 85 dB(A). Provisions should be incorporated to furnish the same protection to those who wear glasses.[5908, 0700]

10.2.1-10 Loudspeakers for Multi-Channel Monitoring

When several channels are to be monitored simultaneously by means of loudspeakers, the speakers should be mounted at least 10 degrees apart in the horizontal plane frontal quadrant, ranging radially from 45 degrees left to 45 degrees right of the user's normal forward facing position.

Additional Information: When additional channel differentiation is required, apparent lateral separation should be enhanced by applying low-pass filtering (frequency cutoff, Fc = 1,800 Hz) to signals fed to loudspeakers on one side of the central user position. If there are three channels involved, one channel should be left unfiltered, a high pass filter with 1,000 Hz cutoff should be provided in the second channel, and a low-pass filter with 2,500 Hz cutoff should be provided in the third channel. A visual signal should be provided to show which channel is in use.[5908]

10.2.1-11 Volume Controls

Accessible volume or gain controls should be provided for each communication receiving channel (e.g., loudspeakers or headphones) with sufficient electrical power to drive sound pressure level to at least 100 dB overall when using two earphones.

Additional Information: The minimum setting of the volume control should be limited to an audible level; i.e., it should not be possible to inadvertently disable the system with the volume control. While separation of power (on-off) and volume control adjustment functions into separate controls is preferred, should conditions justify their combination, a noticeable detent position should be provided between the OFF position and the lower end of the continuous range of volume adjustment. When combined power and volume controls are used, the OFF position should be labeled. Speaker volume should be adjusted to ensure that speaker communications will not prevent detection of other audio signals, e.g., alarms.[5908, 0700]

10.2.1-12 Squelch Control

When communication channels are to be continuously monitored, each channel should be provided with a signal-activated switching device (squelch control) to suppress channel noise during no-signal periods. *Additional Information:* A manually operated on-off switch should be provided to deactivate the squelch when receiving weak signals.[5908]

10.2.1-13 Periodic Maintenance Tests

Periodic tests should be performed on all communication systems to ensure that messages remain intelligible under changes in ambient noise levels that may have occurred since the last check.[0700]

10.2.2-1 Handset Size and Shape
The size and shape of handsets should be compatible with user's hand size and mouth-ear distance (standard telephone dimensions are acceptable).[0700]

10.2.2-2 Handset Design
Handset earpieces should maintain firm ear contact while the transmitter is positioned in front of the mouth.[0700]

10.2.2-3 Retractable Handset Cords
Cords should be of nonkink or self-retracting type.[0700]

10.2.2-4 Handset Cord Length
Cords should be of sufficient length to permit reasonable user mobility.[0700]

10.2.2-5 Handset Cord Position
Cords should be positioned so as to avoid entangling critical controls or endangering passing traffic.[0700]

10.2.2-6 Handset Cradles
Vertically mounted handset cradles should be designed and located to prevent the handset from being knocked out of the cradle by passing traffic.[0700]

10.2.2-7 Multiple Instruments
Where multiple telephone instruments are located close together (e.g., on a single desk), they should be coded to indicate circuit or function.[0700]

10.2.2-8 Press-to-Talk Button
If a press-to-talk button is used, the button should be convenient to both left-and right-hand operation.[0700]

10.2.2-9 Switching Mechanism
Switching should be designed and/or programmed to minimize delay in making desired connections under both normal and emergency conditions.
Additional Information: Usually the switching function is accomplished by dial switching, and the switching mechanism is located in-plant. Switching should be programmed to give the control room automatic priority of access to the switching system.[0700]

10.2.2-10 Telephone Ringing
The volume of ringing should be adjustable at the individual telephone instrument.[0700]

10.2.2-11 Announcing Use
The transmitter should be compatible with the rest of the announcing system when used as the microphone input to the announcing system.[0700]

10.2.3-1 Feedback

Within engineering constraints imposed by sound-powering, the system should provide in-phase feedback to the user.

Additional Information: In control room use, sound-powered phones are generally of the headset variety (either one or two earphones and a boom microphone in an assembly fitting on the head). Sound-powered phones are independent of external power, a feature of value in emergency use. Additionally, the headset configuration, used with conveniently located plug-in jacks, provides mobility for the user when moving to remote locations (back panels or outside the control room).[0700]

10.2.3-2 Ringing

If ringing is not installed, the user should be able to switch the sound-powered transmitter to the paging system so that a desired party can be called to the line.

Additional Information: Sound-powered phones require supplemental power, which is often hand-generated, to energize a ringing function. Often sound-powered phone circuits have no provision for ringing. Need for ringing must be determined for the individual plant depending on the sound-powered phone procedures.[0700]

10.2.3-3 Jack Provisions

Plug-in jacks for the sound-powered system should be provided within the control room.

Additional Information: Jacks should be located close to the workstations to prevent the need for unduly long cords. Jacks should not accommodate plugs of the conventionally powered phone system, in order to avoid wrong instrument-system connections.[0700]

10.2.3-4 Switching

When used, patch panels should be conspicuously marked and located in reasonably accessible places.

Additional Information: These requirements are particularly critical in back-panel areas. A complete set of cords should be provided at each panel if cord-type patching is used. The requirements for switching must be assessed for the individual plant depending on procedures for use of sound-powered phones.[0700]

10.2.3-5 Cushioning of Earpieces

Earphone cushioning to provide comfort for extended periods of wear.[0700]

10.2.3-6 Fit of Earpieces

Earpieces should cover the outer ear without causing uncomfortable pressure.[0700]

10.2.3-7 Fit of Headsets

The headset should be held firmly in place, yet be easy to remove[0700]

10.2.3-8 Storage of Headsets

A well-marked and accessible place should be provided for headset stowage[0700]